ACCESS Stereo BRIC IP Codec

You'll be seeing me from time to time throughout this manual to point out ACCESS advanced topics. Feel free to ignore these sections as the default settings provide good performance for most users.

Table of Contents

Table Listing

Figure Listing

About Comrex

Comrex has been building reliable, high quality broadcast equipment since 1961. Our products are used daily in every part of the world by networks, stations and program producers.

Every product we manufacture has been carefully designed to function flawlessly, under the harshest conditions, over many years of use. Each unit we ship has been individually and thoroughly tested.

Comrex stands behind its products. We promise that if you call us for technical assistance, you will talk directly with someone who knows about the equipment and will do everything possible to help you.

You can contact Comrex by phone at 978-784-1776. Our toll free number in North America is 800-237-1776. Product information along with engineering notes and user reports are available on our website at www.comrex.com. Our email address is info@comrex.com.

Warranty and Disclaimer

All equipment manufactured by Comrex Corporation is warranted by Comrex against defects in material and workmanship for one year from the date of original purchase, as verified by the return of the Warranty Registration Card. During the warranty period, we will repair or, at our option, replace at no charge a product that proves to be defective, provided you obtain return authorization from Comrex and return the product, shipping prepaid, to Comrex Corporation, 19 Pine Road, Devens, MA 01434 USA. For return authorization, contact Comrex at 978-784-1776 or fax 978-784-1717.

This Warranty does not apply if the product has been damaged by accident or misuse or as the result of service or modification performed by anyone other than Comrex Corporation.

With the exception of the warranties set forth above, Comrex Corporation makes no other warranties, expressed or implied or statutory, including but not limited to warranties of merchantability and fitness for a particular purpose, which are hereby expressly disclaimed. In no event shall Comrex Corporation have any liability for indirect, consequential or punitive damages resulting from the use of this product.

Section 1 Introduction

Congratulations on purchasing the Comrex ACCESS codec. This product is the next step in the evolution of audio transportation over networks. For Comrex, this began in 1976 with the introduction of the Frequency Extender, followed by ISDN codecs in the early 1990s and POTS codecs in 1996. So we've been doing this for a long time.

The ACCESS product is the result of years of our research into the state of IP networks and audio coding algorithms. This has all been in the quest to do what we do best, which is to leverage existing, available services to the benefit of our core customers - radio remote broadcasters.

The heart of this product is called BRIC (Broadcast Reliable Internet Codec). While others have introduced hardware coined "IP Codecs," this is the first product we're aware of that dares to use the word Internet "with a capital I." Given the challenges the public Internet presents, it's no small boast to say that this product will perform over the majority of available connections.

BRIC represents a change that is both desirable and inevitable for remotes. It's inevitable because, as available connections move from old fashioned "circuit switched" style to newer "packet switched" style, technology like ISDN and POTS codecs will begin to work less and less often. The desirability stems from the new wireless networks that will make remote broadcasting more mobile, simpler and less expensive. BRIC technology has been engineered not only to be robust enough for the Internet, but usable in really challenging Internet environments like 802.11x Wi-Fi, Wi-Max, 3G cellular and satellite based Internet connections.

Those of us here who have been remote broadcasters have been wishing for a system like this for a long time. As former broadcasters turned designers, it's our hope that this kind of enabling technology will tickle the imagination of the user, enabling more creative and entertaining programming to be broadcast from more diverse and interesting locations. Please let us know about your unique ideas and adventures by dropping us a note at techies@comrex.com.

ABOUT BRIC

BRIC (Broadcast Reliable Internet Codec) is a breakthrough technology with hardware that will deliver audio over the public Internet in much the same way that ISDN and POTS codecs have performed in the past. BRIC consists of three pieces:

- Rackmount ACCESS codec (which you are using)
- Portable ACCESS codec
- Switchboard Traversal Server

We will describe each piece independently:

1) Rackmount ACCESS codec — This product is designed for installation in a radio station's "remote rack" and is designed for "always on" operation. Hence the lack of a power switch. Also, it is envisioned that this product will be controlled entirely from a computer connected to the local LAN. There are no user controls on the ACCESS Rack (other than a recessed reset button) and the only indications are audio meters and a **Ready** light to indicate an incoming data stream. After initial configuration, all connection, status and diagnostics are available via the internal web server and Console Connection Interface.

2) Portable ACCESS codec — This product is engineered to provide the most convenience for the remote broadcaster on the road. It combines small size, battery power, clip-on mixer and headphone drivers with an audio codec capable of remarkable quality on the public Internet.

3) Switchboard Traversal Server — This server exists on the public Internet at a fixed address and performs several functions. Its use is optional but makes connections between ACCESS codecs much simpler and removes worries about dynamic IP's, NATs, and other concerns that can make peer-to-peer connection over the Internet difficult (especially over tightly controlled networks like 3G or Wi-Fi). The Switchboard TS provides the following functions:

a) Communicates with all ACCESS codecs that are provisioned to work with it. It keeps a log of the IP address of every codec that wishes to be subscribed.

b) Maintains a "keep alive" channel to each codec subscribed, allowing Traversal of firewall and Network Address Translators when receiving an incoming call.

c) Provides each subscribed ACCESS codec with a "Buddy List" of other users, their current status, and will facilitate connection to them if desired.

More About ACCESS Rack

ACCESS Rack incorporates all the features, algorithms and services of BRIC as defined in the previous sections. Its main function is to provide a robust, high quality, low-delay audio link in full-duplex over challenging IP networks like the public Internet. To this end, it provides an intuitive and attractive *Web-based Interface* via web-browser and a direct connect *Console Connection Interface*. Using these interfaces, you can select operating modes, check audio levels, make and end connections, and check network statistics of any connections you make. While ACCESS is designed to handle most network challenges in its default configuration, advanced options are available to allow customization of parameters that have effect on link stability and delay.

But wait! There's more! ACCESS is also a POTS codec. It has a built-in modem which can be set to make calls over analog phone lines directly to other units. In this mode, ACCESS can communicate with other ACCESS devices, or with a range of previous generation POTS codec devices made by Comrex.

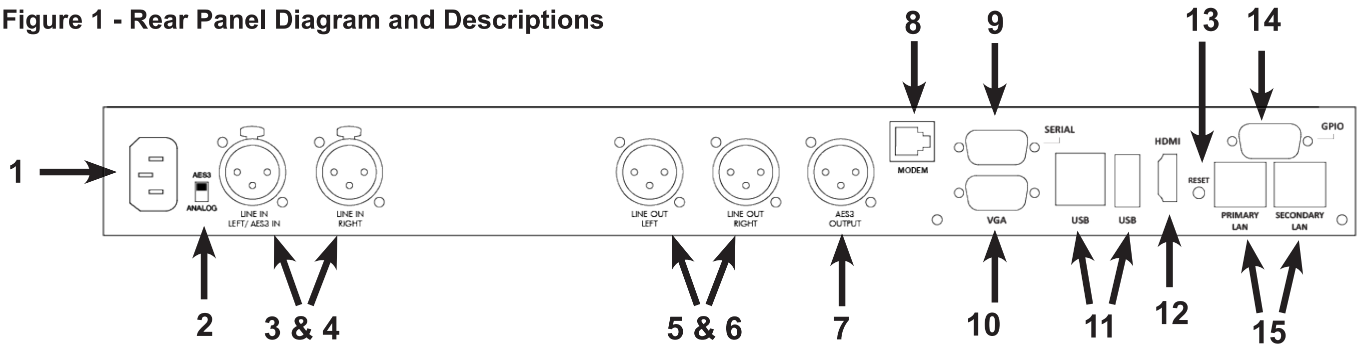
What Comes With ACCESS Rack

The following items are shipped with a new ACCESS Rack:

(1) ACCESS Stereo BRIC IP Codec (Rackmount)
(1) 6' Ethernet cable
(1) 6' Telephone cable
(1) AC Power cord
(1) Operating manual
(1) Warranty card (Please fill out and return)

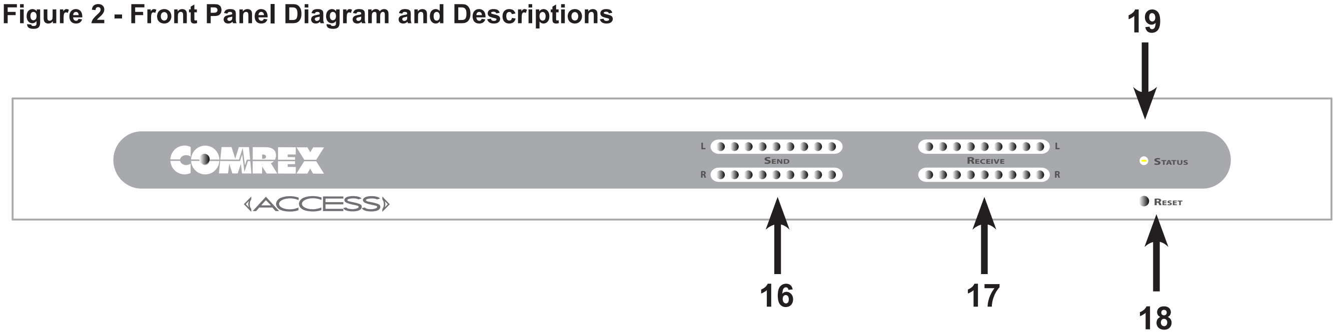
SECTION 2 RACK DIAGRAMS AND INSTALLATION

Figure 1 - Rear Panel Diagram and Descriptions



1) AC INPUT	This is an IEC connector for the main power. ACCESS works on worldwide AC power at 110-240VAC 50-60Hz, auto detecting.
2) Analog/AES3 Input Switch	This switch determines whether the Line In Left/AES3 In XLR connector is used for analog or AES3 digital audio input.
3) AND 4) ANALOG AUDIO INPUT	Apply balanced analog audio to be sent over the network here. Left channel is used for mono encoding modes. Level is set to 0dBu (0.775VRMS) nominal. Full scale input is +20dBu.
5) AND 6) ANALOG AUDIO OUTPUT	Balanced analog audio is available at these ports. Level is set to 0dBu (0.775VRMS). Full scale output is +20dBu.
7) AES3 DIGITAL AUDIO OUTPUT	A 48KHz AES3 stereo signal is available here. AES3 output is available simultaneously with analog. When the AES3 Input is active, the AES3 Output will lock to the sampling rate and clock signal of the Input.
8) POTS/PSTN	Attach an analog telephone line here for POTS codec compatibility.
9) SERIAL PORT	Asynchronous ancillary data is available here.
10) VGA OUTPUT	Attach a VGA computer monitor here for accessing the *Console Connection Interface*.
11) USB PORTS	Available for use with USB keyboards and mice. May also be used with some 3G/4G/Wi-Fi adapters.
12) HDMI OUTPUT	Attach an HDMI compatible monitor here for accessing the *Console Connection Interface*.
13) RESET	This button will restart the Rack's computer board.
14) CONTACT CLOSURES	Four sets of contact closure inputs and outputs are available on this port. These can be used to send signals to the far end of the link or to trigger remote control gear such as automation equipment.
15) ETHERNET PORTS	1000Base-T Ethernet ports for connection to your network.

Figure 2 - Front Panel Diagram and Descriptions



16) Send — Peak meter that displays the level of audio being sent locally into the ACCESS, regardless of whether or not a connection is active. Proper level is indicated by peaks driving the **Yellow LEDs**, while avoiding lighting the **Red LEDs** (which indicates clipping).

17) Receive — Peak meter that displays the level of audio being sent remotely when a connection is active. Proper level is indicated by peaks driving the **Yellow LEDs**, while avoiding lighting the **Red LEDs** (which indicates clipping). Adjustments to this level must be made on the far end of the link.

18) Reset — Recessed button to send ACCESS into hardware reset mode. Approximately 30 seconds are required to reboot when this is pressed.

19) Status — Indicates several states of **Ready**:

Off = Network ready, not connected to remote
Red = Network unavailable
Green = Connected to remote
Yellow = Connected to remote but no network (i.e. network connectivity lost during connection)
Slow Red Blink = Software update in progress
Fast Red Blink = Displaying unit IP address

Mono vs. Stereo — ACCESS uses its left channel input only for *Mono Modes*. Right channel is ignored. Output audio is available at both the left and right outputs in *Mono Mode*.

Pinouts - Audio — ACCESS audio connections are balanced professional level inputs and outputs.

Table 1 - XLR Pinout

Pin 1	Ground
Pin 2	Audio +
Pin 3	Audio –

Table 2 - AES3 Pinout

Pin 1	Ground
Pin 2	Data +
Pin 3	Data –

PINOUTS - CONTACT CLOSURE

Contact closures are available via the male 9-pin D connector on the back of the ACCESS Rack. Inputs are triggered by shorting the respective input to **Pin 5**. Outputs consist of an *open collector* circuit which, when inactive, will offer a high-impedance path to **Pin 5** and, when active, will offer a low impedance path to **Pin 5**. These outputs are capable of sinking up to 200mA at a voltage up to 12V. Do not switch AC mains power using these contacts.

Table 3 - Contact Closure Pinouts

Pin 1	Input #1
Pin 2	Input #2
Pin 3	Input #3
Pin 4	Input #4
Pin 5	Ground
Pin 6	Output #1
Pin 7	Output #2
Pin 8	Output #3
Pin 9	Output #4

PINOUTS - SERIAL PORT

The **Serial Port** is capable of transferring ancillary data to the far end of the connection. By default, the communication parameters are set for 9600bps, no handshaking, no parity, 8 data bits, one stop bit (9600,n,8,1). It is pinned on a 9-pin D female in DCE-style pinning. The port is designed to connect to a 9-pin PC serial port with a straight-through M-F cable. RS-232 levels are used.

Table 4 - Serial Port Pinouts

Pin #	**Function**	**Direction**
1	CD	Unused
2	RX Data	From ACCESS
3	TX Data	To ACCESS
4	DTR	To ACCESS
5	Ground	
6	DSR	From ACCESS
7	RTS	To ACCESS
8	CTS	From ACCESS
9	RI	Unused

SECTION 3 SETTING UP ACCESS

HOOKING UP

At a minimum, ACCESS will need an audio connection and a network connection. Levels of all analog audio I/O is 0dBu (0.775V) nominal. This level will provide 20dB headroom before the clipping point. Input audio is reflected on the front panel LED based peak meters. Clipping is indicated by the **Red LED** on these meters.

ABOUT NETWORK CONNECTIONS

ACCESS needs a network connection to be useful. On ACCESS Rack, the network connection is made via a standard 10/100baseT Ethernet connection on an RJ-45 connector.

In most ways, ACCESS will look like an ordinary computer to this network. In fact, ACCESS contains an embedded computer with a Linux-based operating system and a full network protocol stack.

ACCESS is perfectly capable of working over most LANs, but there may be situations where a LAN is heavily firewalled, subject to overloaded traffic conditions, or have security concerns. Better performance is possible if ACCESS has its own Internet connection. Often, it's worth the trouble to install a DSL line especially for ACCESS, especially if the cost is reasonable.

Since there may be bandwidth, firewall, and security concerns with installing ACCESS on a managed LAN, it is recommended that your IT manager be consulted in these environments. The details that follow assume a working knowledge of IT topics and network configuration.

SETTING UP ACCESS NETWORK CONNECTIONS

We recommend putting ACCESS on a LAN and scoping out its functions before use. To do this, ACCESS must be given an IP address. This is the Internet location where you can connect to ACCESS through a web browser. It will also be the address used when another ACCESS is connecting to it.

Every device on an IP network must have a unique IP address. This is a number between 0 and 4,294,967,295, which is the range of values that can be represented by 32 binary bits. For simplicity, we break this 32-bit value into four eight-bit values and represent each as a decimal number (between 0-255) separated by dots. For example, the Comrex test IP number is 70.22.155.131.

A device with a public Internet connection can either have a public IP address (which is directly accessible by the Internet) or a private IP address, which is directly accessible only by the LAN on which it is connected.

Figure 3 shows connection of an ACCESS directly to the Internet using a public IP address. Figure 4 shows connection to a subnet (or LAN) using a private IP address, with a gateway router separating the LAN from the public Internet.

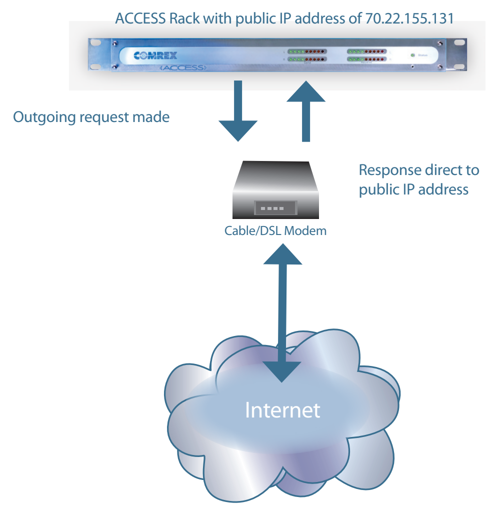


Figure 3 - Direct connection to Internet

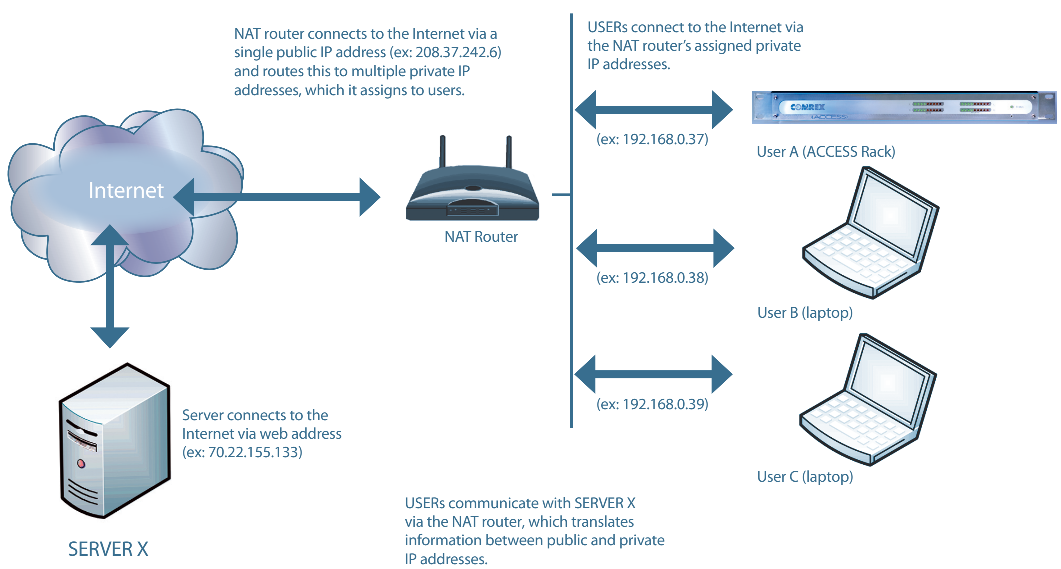


Figure 4 - Connection to Internet via subnet (or LAN)

To have the ability to make connections normally, without using the traversal functions of the Switchboard Traversal Server (Switchboard TS), one of the ACCESS in the link should be connected to a public IP address. This can be achieved several ways:

> 1) ACCESS can be the only device connected directly to its Internet link or it can share an Internet link that provides more than one IP address.
> 2) ACCESS can be connected behind a NAT router, which can be programmed to provide public Internet access to it through port forwarding.

But for now we'll assume you have a way to set up at least one end of your ACCESS link with a public IP. In a radio remote environment, this should probably be the studio end, since you will often have much less control on the remote side.

Dynamic vs. Static Addressing

ACCESS can be set to its own, fixed IP address (referred to as *Static* in Internet-speak) or can obtain its address from the network (known as *Dynamic* or DHCP). This concept is entirely independent from the *Public vs. Private* concept. Public and private addresses can each be dynamic or static.

Dynamic (DHCP) — ACCESS is set by default to DHCP addressing, meaning that it looks to your network for assignment of an IP address. If your network has a DHCP server and this is the way you intend to use it, you don't need to alter any settings in the *Console Connection Interface*. You will, however, need to know what address is being assigned to ACCESS by the network. This is easily done by attaching a computer monitor to the VGA port on ACCESS before applying power. After ACCESS boots, it will display the current IP address on the monitor. Note: DHCP addresses can change over time, so you may need to recheck the address if you are having trouble connecting.

Finally, there's one other way to determine the IP address of ACCESS. If you're unable to put a computer monitor on the system, you can infer the IP address by what's displayed on the front panel LEDs for a few seconds during the boot process.

DHCP servers typically assign IP address in a standard format. This is because they must choose addresses that are not in use by the Internet at large. They will likely choose an address at one of 3 distinct ranges:

192.168.x.x	172.16.x.x	10.x.x.x

Also, on 192.168 style and 172.16 style subnets, the third entry will typically be a single digit (often 0 or 1). You can usually find out the DHCP assignment style by querying a Windows computer on the same LAN using Run->Cmd->ipconfig. If you know your DHCP server assigns addresses using one of the first two formats (or you know the DHCP assignment range on a 10.x.x.x network) you can usually derive the true IP address by the front panel LEDs. They will display a "coded" version of the IP address assigned for a few seconds during boot just before the ACCESS enters operational mode. During this time, the **Ready** light on the front panel flashes quickly, and the **Level LEDs** display the last 4 digits of the IP address. This is best shown by example:

Assume you are using a Linksys router on your network that has a built-in DHCP server. You may be aware that by default this router assigns IP addresses using the range 192.168.1.2-255. Let's assume that when connected, the ACCESS is assigned an IP address of 192.168.1.7. The **LEDs** will display the last four decimals of this address (including zeros) so during boot you will see the following code:

L Send will display 1 LED
R Send will display 0 LEDs
L Receive will display 0 LEDs
R Receive will display 7 LEDs

You can now assume that your ACCESS has the address of 192.168.**1.007**

Static IP — Setting a Static IP requires that you enter some details into the ACCESS. You will need to enter the following information via the *Console Connection Interface*:

- **IP address of the ACCESS** – make sure this has been provided by your ISP or that nobody else on your LAN is using this address.
- **Subnet Mask** – A series of numbers that indicate the range of your LAN addresses. If in doubt, try 255.255.255.0.
- **Gateway Address** – The address of the Internet gateway on your account. If in doubt, try the first three number of your IP address with the last digit of 1 (e.g. xxx.xxx.xxx.1).

More details on how to input this information are contained in the next section.

SECTION 4 GAINING ACCESS TO ACCESS VIA THE CONSOLE CONNECTION INTERFACE

The use of the *Console Connection Interface* is required when configuring the IP parameters. It also provides access to many of the features found in the *Web-based Interface*. We'll cover the *Console Connection Interface* here, and the *Web-based Interface* in later sections.

Using the *Console Connection Interface* requires that you attach a PS/2 or USB style keyboard and video monitor to the appropriate jacks on the rear panel of ACCESS Rack. You may also attach an USB or PS/2 style mouse to make navigation easier. When using the PS/2 style keyboard or mouse remove and re-apply power after connection.

Top and Bottom Navigation Bars

As shown in Figure 5, all menus on the *Console Connection Interface* contain the top and bottom navigation bars, which contain shortcuts to various setup and status displays. The top bar contains four tabs:

- **Network –** Enable and disable the Ethernet Port or POTS Modem. Configure IP parameters.

- **Remotes –** Create and configure the addresses and profiles of the various outgoing connections. Essentially, this creates an editable "phone book" of places you connect to.

- **Stats –** View network performance data of active connections

- **Configure –** Create profiles for outgoing connections, manage how incoming connections are treated, and change configurations of additional features like audio switching, contact closures and incoming password security.

The bottom bar contains the following shortcuts:

• **Pickboard** – Allows use of the pop-up keyboard for text entry and eliminates the use of a PS/2 or USB style keyboard.

• **Chat** – Jumps immediately to the chat screen/pickboard, allowing text messaging to other ACCESS users.

• **F1/Arrow/Enter** – As shown in the legend on the bottom of the page, the **F1** key on the keyboard provides access to the pull-down menus and the **Arrow** and **Enter** keys are used to navigate.

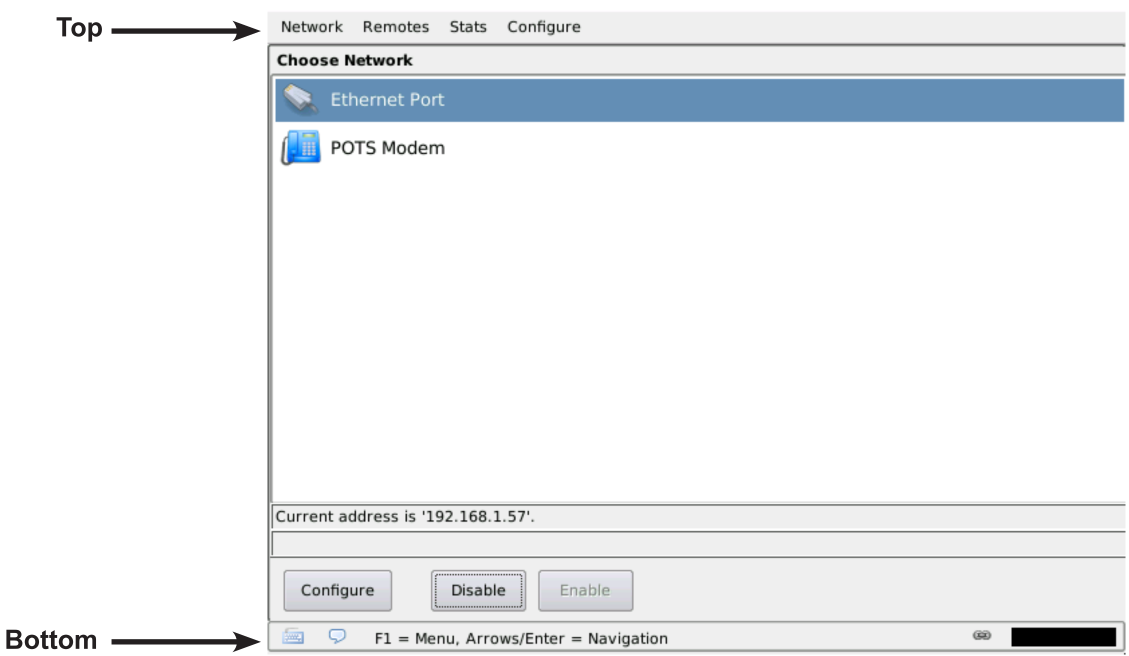


Figure 5 - Top and Bottom Navigation Bars

Network Tab

The **Network Tab** is shown in Figure 5. The Ethernet port and POTS modem may be individually enabled and configured via this interface.

Network Tab - Ethernet Port Set-up

The main tab of interest in configuring the Ethernet port is shown in Figure 6, the **TCP/IP Tab**. Use the drop down menu to select one of the four configuration options for Ethernet **- Static, DHCP, PPPoE, Gateway**.

For DHCP (Dynamic) connections, simply select **DHCP** and the unit will automatically obtain the network settings.

If your connection requires a static, or fixed IP address, you can enter that along with your subnet mask and gateway information in the appropriate fields. If you know the address of your DNS server, enter it here. This is required for use of Switchboard TS and the internal browser functions.

PPoE (Point-to-Point Protocol over Ethernet) is used by some DSL and WiMAX services to establish and end sessions much like a dial-up modem does. Most IP connections don't use it and it can usually be ignored.

If your ISP requires PPoE session to be established, rather than entering IP information you may enter a user name and password to establish connection. These are supplied by your ISP.

PPoE connections always use dynamic IP addressing. When using PPoE an IP address will be assigned by the DHCP server at the ISP and will appear on the bottom bar of the network menu.

The **Gateway** option is an advanced topic and is described in the *Gateway Operation* section. It should not be enabled for most applications.

After the Ethernet parameters are set, you may enable the Ethernet port. For DHCP connections, this will prompt ACCESS to acquire an IP address from the DHCP server. Enabling and disabling the Ethernet port is equivalent to "releasing" and "renewing" IP addresses. The acquired IP address will appear on the bottom bar of this display.

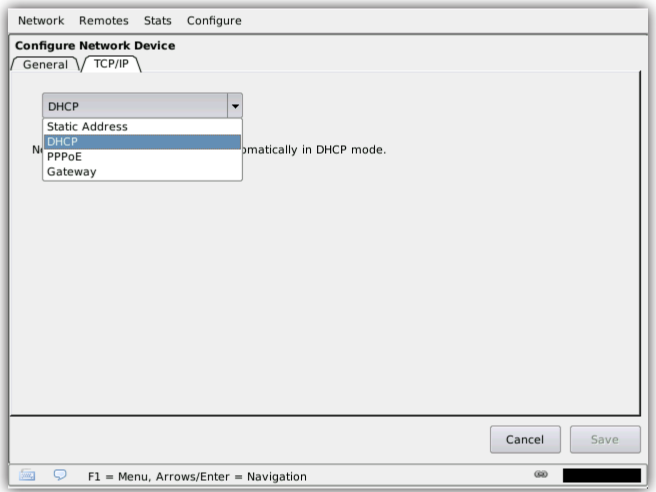


Figure 6 - TCP/IP Tab for Ethernet Port Configuration

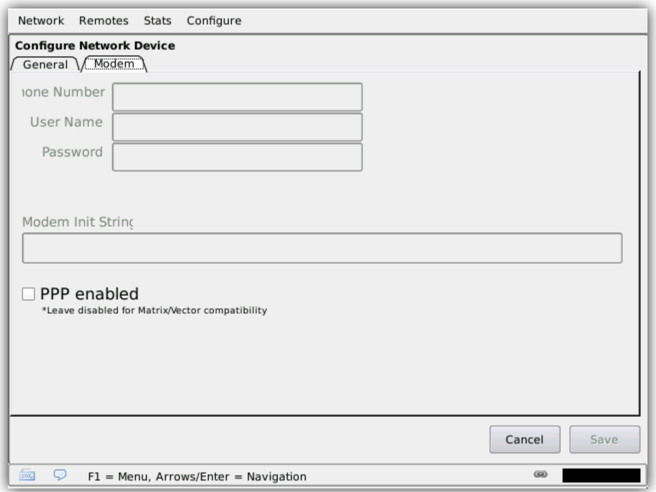


Figure 7 - POTS Modem Configuration Tabs

NETWORK TAB - POTS MODEM SET-UP

The modem in the ACCESS can be configured for either *Non-PPP Mode* or *PPP Mode*, as shown in Figure 7. Most users may leave the default settings.

Non-PPP (POTS Codec) Mode is the default setting. This is used to place a call to another codec directly over the telephone line with no Internet Service Provider involved. This is the only mode available to connect to other Comrex POTS codecs. Because of the narrow bandwidth of dial-up Internet connections, use of *POTS Codec Mode* is strongly preferred over modem *PPP Mode*. No options are available for *Non-PPP Mode*. The extra modem init string for this mode is done in the **System Settings Tab** (the **Advanced** box must be selected in order for this option to appear).

PPP Mode allows the use of a dial-up Internet Service Provider. Configure your ACCESS with your ISP information. The ACCESS will function like an IP codec over the link, connecting to other ACCESS IP addresses.

PPP Mode should only be used when connecting to an Internet Service Provider via the modem. In this mode, you will need to enter the phone number, user name and password settings provided by your ISP.

Once your ISP parameters are configured, you may enable the modem and the call to your ISP will be dialed automatically. This call will be maintained until the modem is disabled in the **Network Tab**.

Connections in this mode are placed in the same way that normal IP connections are placed. A remote connection must be built using one of the non-POTS based profiles and the address must be an IP address.

PPP Mode depends on the modem connect rate and many codec profiles will not fit within the PPP channel. We recommend use of the *ULB Mode* for most reliable connections over modem PPP.

Web Browser

This option will open a graphical web browser and allow you to test your Internet connection by looking at a web page. This browser does not support Flash and other complex protocols, but is suitable for basic Internet use. The browser is also helpful in scenarios where the local LAN requires that users log-in via a web based security page (as in many hotels). The browser does not have a "close" button, but the socket it creates will close automatically when an audio connection is made.

Remotes Tab

The **Remotes Tab** (shown in Figure 8) is the first screen to appear when the system is turned on. It allows you to define and edit your outgoing connections, as well as indicate the presence of incoming connections.

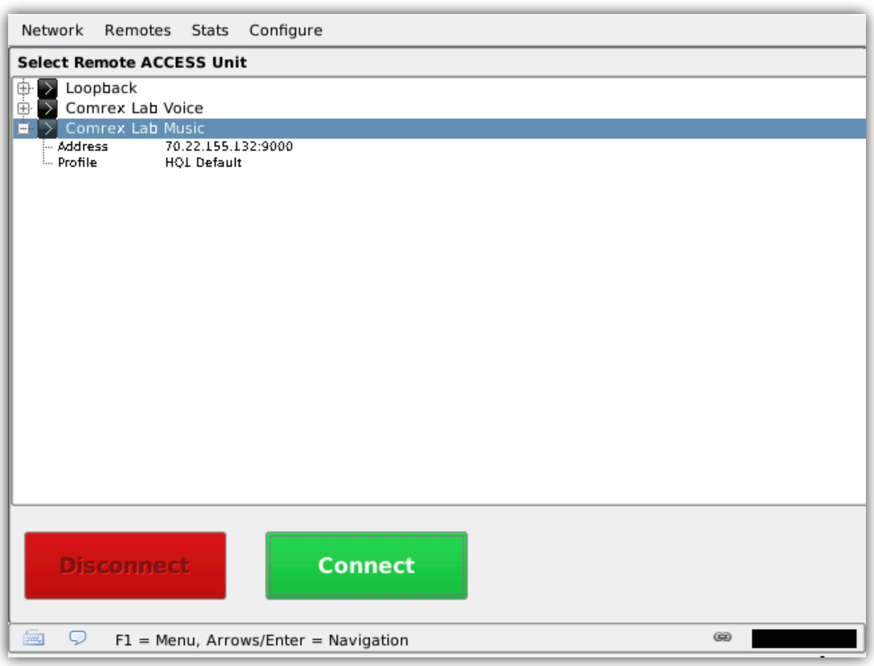


Figure 8 - Console Connection Interface Remotes Tab

This section describes how to enter “local” remotes into the product to dial them by IP address. If you plan on using the Switchboard Traversal Server, or take only incoming calls, this step may not be necessary. For more information on Switchboard Traversal Server, see Section 10.

By default, three remotes are already present on the **Remotes Tab**, and can be used immediately for testing. You may add to this list by pulling down the **Remotes** menu and selecting **Add New Remote**. This display is shown in Figure 9. You will need to input a name for this remote (which can be anything), as well as the destination IP address (or phone number for a POTS call). Finally, you must choose one of the pre-defined profiles to dictate how each direction of the connection behaves. Several factory defined profiles exist for commonly used configurations, and you can create your own (described in the *Console Connection Interface* CONFIGURE TAB section).

Optionally, you may add a password to this outgoing remote for connection authentication. In this case, the incoming ACCESS must also be programmed with the matching incoming password.

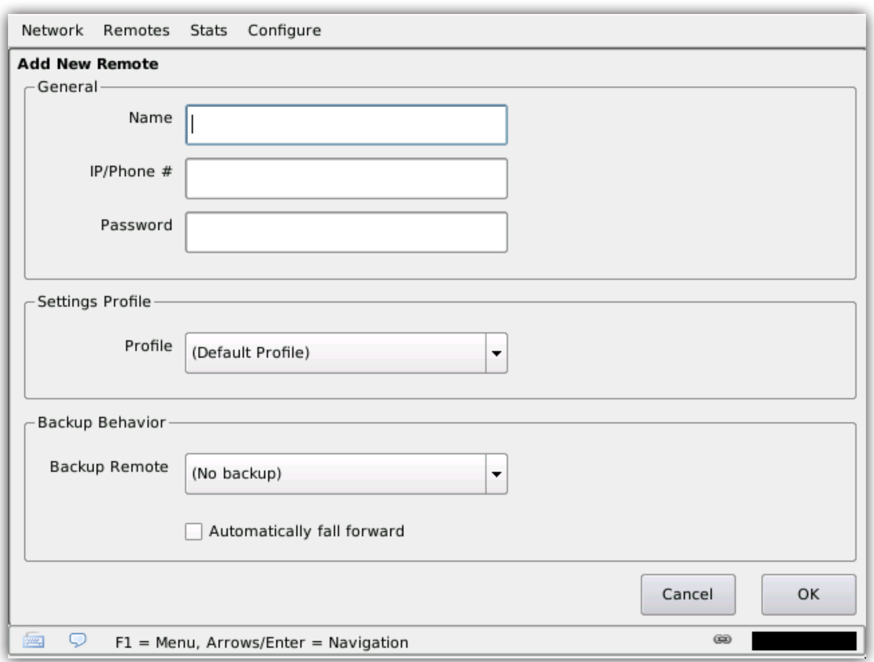


Figure 9 - Add New Remote Screen

Finally, you may specify how the unit is to behave when connection is lost to this remote (see *Backing Up a Connection* in the *Web-based Interface* section).

Once a connection is added, it will appear in the main remotes list. Return to the list by selecting **Remotes** and then **Manage Connections**. If you expand your chosen remote with the **+** option, the system will display the destination IP address and the profile for that remote. Remotes will remain in this list until they are deleted or the configuration of the entire system is reset.

Existing remotes may be edited by highlighting one and selecting **Remotes** and then **Change Remote Settings.**

Incoming connections are displayed by their IP address, or, if also configured as outgoing connections, by their names. Incoming POTS connections are displayed as “incoming”.

To make a connection, be sure your network is configured and enabled in the **Network Tab**. Then, from the **Remotes Tab**, simply select an outgoing connection and choose **Connect**. Choose **Disconnect** to end a connection.

STATS TAB

ACCESS provides lots of information on the **Stats Tab** about network performance. This information is divided into C**hannel Stats**, which provides information about all incoming and outgoing data, and **Peer Stats**, which gives detailed information regarding the decoder buffer manager's functions. Both sets of information are available on a text-tree basis, as well as graphical real time charts showing historical performance.

As shown in Figure 10, the **Channel Stats** provide real-time graphs of outgoing and incoming packets. Each column represents one second of outgoing data, segmented into audio coding data (blue) and overhead like IP/UDP headers, RTP headers etc (light blue).

The *Numeric Channel Stats* tab (Figure 11) gives an indication of the same values instantaneously, as well as the total amounts of incoming and outgoing data in bytes for the current connection. This information can be helpful when operating on data networks with per-megabyte transfer charges. If you do not have an unlimited data plan you may want to keep track of overall data usage and optimize your connection profile for the most efficient transfer settings. For additional information on choosing encoding algorithms and other ACCESS settings see *SECTION 16 ADVANCED TOPICS*. These totals reset once the connection is closed.

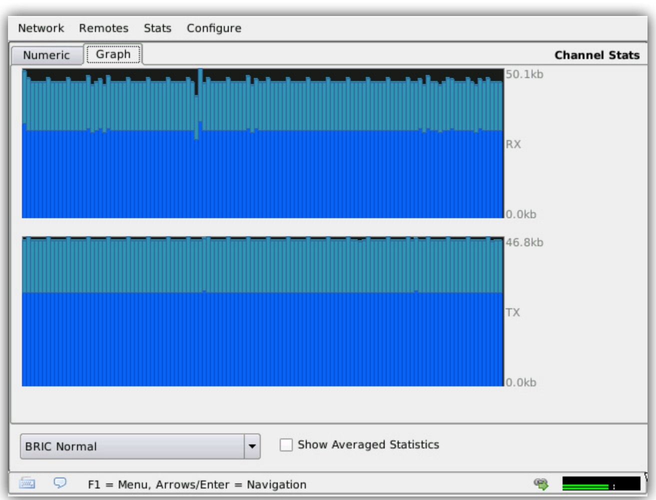


Figure 10 - Channel Stats in Graph Format

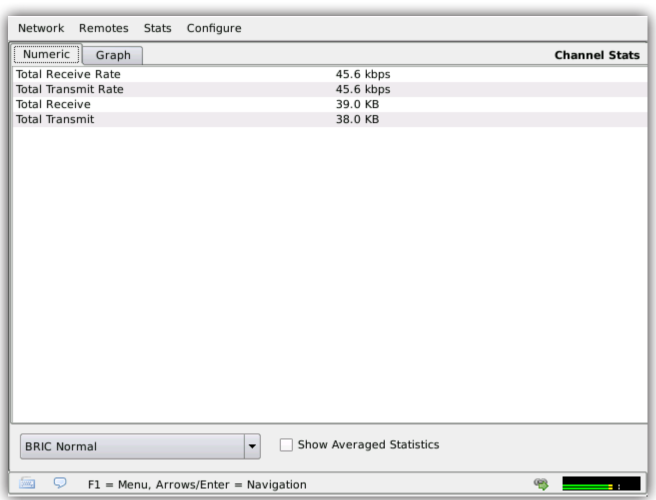


Figure 11 - Channel Stats in Numeric Format

The **Peer Stats** display is shown in Figure 12. The top graph represents the work of the **Jitter Buffer Manager**. The area of most interest is the light blue area as shown in the diagram, which illustrates a spread of jitter values (referenced to the current playout pointer) over the last second. If this area covers a large span, the relative jitter is high. If the light blue section of the graph is small or invisible over a time period, there has been very little jitter present.

Based on the historical value of this jitter figure, the buffer manager will expand or contract the receive buffer (lengthening and shortening overall delay). The time interval over which this measurement is assessed is called the “jitter window” and is adjustable in the **Advanced Profile** editor.

The work of the **Jitter Buffer Manager** is shown by the green line, which is the target buffer delay that the system is trying to achieve, based on measurements done over the jitter window.

The lower half of the **Peer Stats** display shows a real time and historical representation of frame loss. If the decoder does not receive packets in time, the chart will show a red line indicating percentage of lost packets over the one second interval.

The **Numeric Peer Tab** (Figure 13) gives an indication of the same values instantaneously, as well as call duration and other parameters.

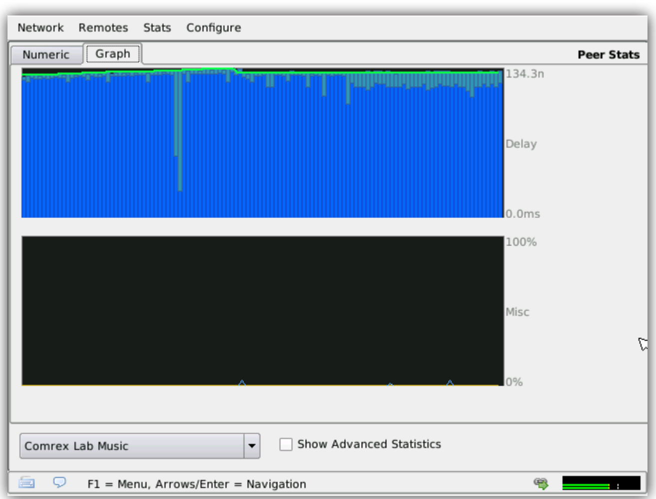


Figure 12 - Peer Stats in Graph Format

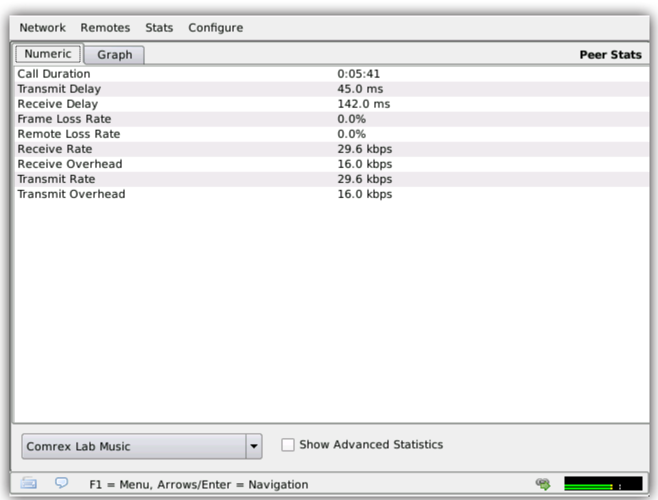


Figure 13 - Peer Stats in Numeric Format

AUDIO LEVEL TAB

The **Audio Level Tab** displays current input and output audio levels in a digital format. The scale may be set for either dBu or dbFS, as shown in Figure 14.

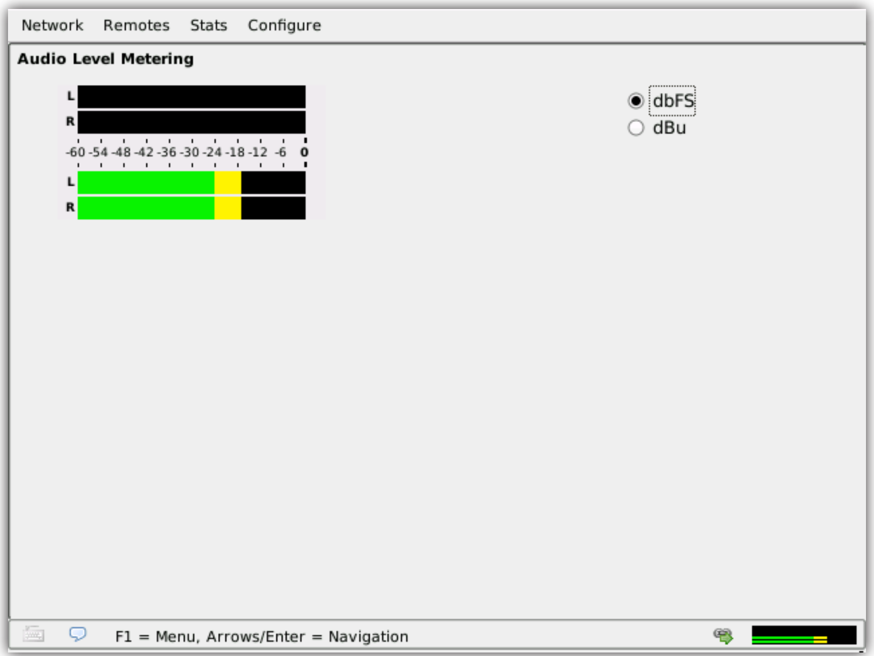


Figure 14 - Audio Metering

CONFIGURE TAB

The **Configure Tab** allows you to set up any global options on ACCESS, as well as create custom profiles to determine the performance of outgoing connections. Since these options are many, they are treated individually in the next section.

The **Configure Tab** offers choices on two layers as shown in Figure 15: the first two commonly used functions followed by additional, less often used functions.

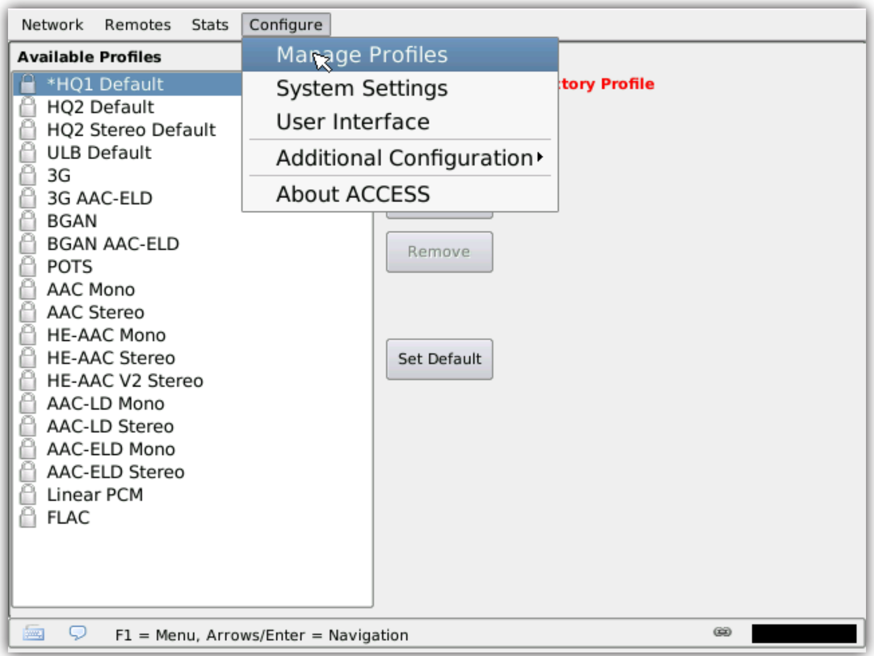


Figure 15 - Configure Tab Pull Down Menu

MANAGE PROFILES

Because ACCESS has many options to optimize individual connections, it includes the concept of **Profiles**, which allow you to define the behavior of a connection in both directions. **Profiles** are separate from the concept of **Remotes**, which define the address to which to connect. A pre-defined **Profile** can be assigned to multiple **Remotes** (and multiple remotes may be defined to the same address which can have different profiles).

ACCESS comes with a series of profiles that are optimized for the majority of IP and POTS connections. Many users may never have the need to define their own profiles. But many advanced options are available to help with troublesome remotes, or remotes with special requirements. In this way, you can build a profile having these advanced options and assign them to one or all remotes you've defined. When using ACCESS, the point where the connection originates controls all available connection parameters in both directions. Keep in mind that these profiles are useful only for connections initiated from the local ACCESS. Incoming connections are defined by the ACCESS at the other end.

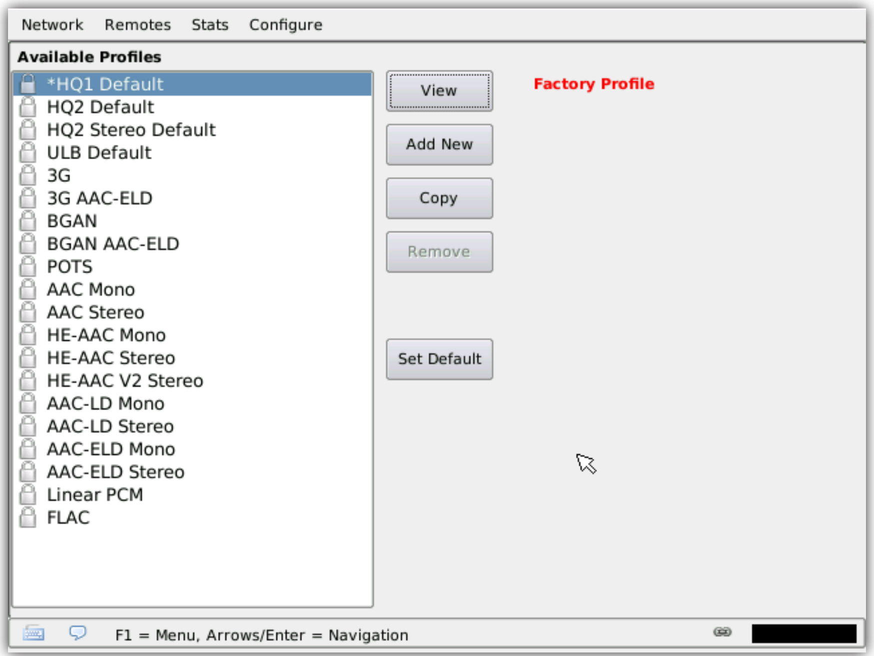


Figure 16 - Available Factory Profiles

Several factory profiles are available and may not be edited by the user. Here's a short description of the proprietary and less known encoding profiles:

HQ1 Default – This is the default choice of profiles for new remotes. It provides a low delay, full duplex, 15KHz mono audio channel over a small (28kb/s) data stream.

HQ2 Default – Although this profile adds substantial additional delay, it is extremely robust and performs well over connections that are prone to packet loss. It provides 15KHz two-way mono audio over small (24kb/s) data streams.

HQ2 Stereo Default – This profile offers a stereo stream using only around 30kb/s. It has the same delay and robustness aspects as HQ2 default above. The stereo stream created needs to have correlation between left and right channels (i.e. you can not send independent programming down each channel).

ULB Default – This profile is best for challenging IP connections. It uses a very small bandwidth stream (14 kb/s) and delivers two-way 7KHz mono voice audio. Not useful for music. For more details, see the algorithms section.

3G – This mode is optimized for use over 3G wireless networks like UMTS, EVDO, and HSDPA. Because 3G networks are usually asymmetrical (they have higher download speeds), this profile delivers a robust, medium delay mono stream in the upload direction, and two, independent low delay mono streams in the reverse direction. These two streams can be useful as separate program and cueing channels, as an example.

BGAN – Profile optimized for use over INMARSAT BGAN terminals. This profile keeps the entire data stream beneath the limit for 32K streaming service, which is the most economical mode for use on ACCESS. This mode provides a robust, medium delay mono stream in the forward direction, and a low delay mono stream in the reverse direction.

POTS – Profile used for connections over the modem card directly to other ACCESS or other Comrex POTS codecs (not through the internet).

Linear PCM – Profile used for sending and receiving Stereo uncompressed audio. Linear PCM requires a large amount of network bandwidth and is generally not suitable for use on the public Internet. Usable in LAN environments (wired or wireless) or with high-speed IP radio links.

FLAC – This profile uses the Free Lossless Audio Codec algorithm for stereo send and receive audio. FLAC can conserve network bandwidth by 30-40% with no loss of audio quality, and only slightly higher delay (when compared to Linear PCM). FLAC still requires a much higher network bandwidth than is available on most public Internet links.

There are several additional factory profiles that use the industry standard AAC Audio Encoders, including: AAC, AAC-LD, HE-AAC & AAC-ELD.

PROFILE SETTINGS

ACCESS provides a powerful set of controls to determine how it connects. The **Profiles Tab** allows you to define one or more profiles to assign to outgoing remote connections. It's often not necessary to define any profiles, since ACCESS ships with a set of default profiles that cover most users. But this tab allows you to build custom profiles to allow for different encoders in each direction, special POTS coding modes, and special options for jitter buffer management. Keep in mind that these profiles are useful only for connections initiated from the local ACCESS. Incoming connections are defined by the ACCESS at the other end.

Profile creation is segmented into commonly used and advanced options. In order to simplify the interface, **Advanced Options** are normally hidden from the user.

Remember, building a profile doesn't change how any remotes are connected until that profile is assigned to a remote on the **Connections Tab**. Once a profile is defined, it will be available on the **Connections Tab** to be assigned to any defined connection.

Building and managing profiles as well as the advanced profile options on the *Console Connect Interface* are similar to using the *Web-Based Interface*. Please refer to the *PROFILES TAB, BUILDING A PROFILE* and *ADVANCED PROFILE OPTIONS* *Web-based Interface* section for complete details.

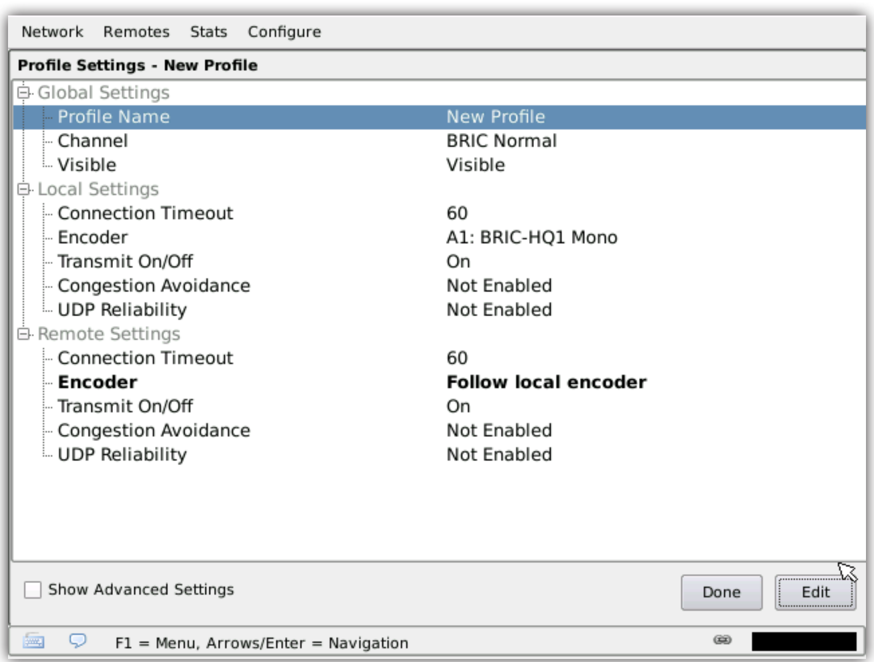


Figure 17 - Profile Settings for a New Profile

System Settings

The **System Settings Tab** defines parameters that are not specific to a particular remote connection. Examples are how incoming (POTS and IP) calls are handled, global modem settings, and how the contact closures are assigned. The **System Settings Tab** is shown in Figure 18.

The **Systems Settings Tab** has nine categories: **System Settings**, **Aux Serial Settings**, **Security Settings, BRIC Normal Settings, HTTP Settings, Modem Settings, Standard RTP Settings**, **N/AICP SIP Settings** and **TCP Settings**. As with the **Profile Tab**, basic options are shown by default. Less used options are hidden until the **Show Advanced Options** box is clicked. All of these settings are explained in detail under the *Web-based Interface System Settings* section of the manual.

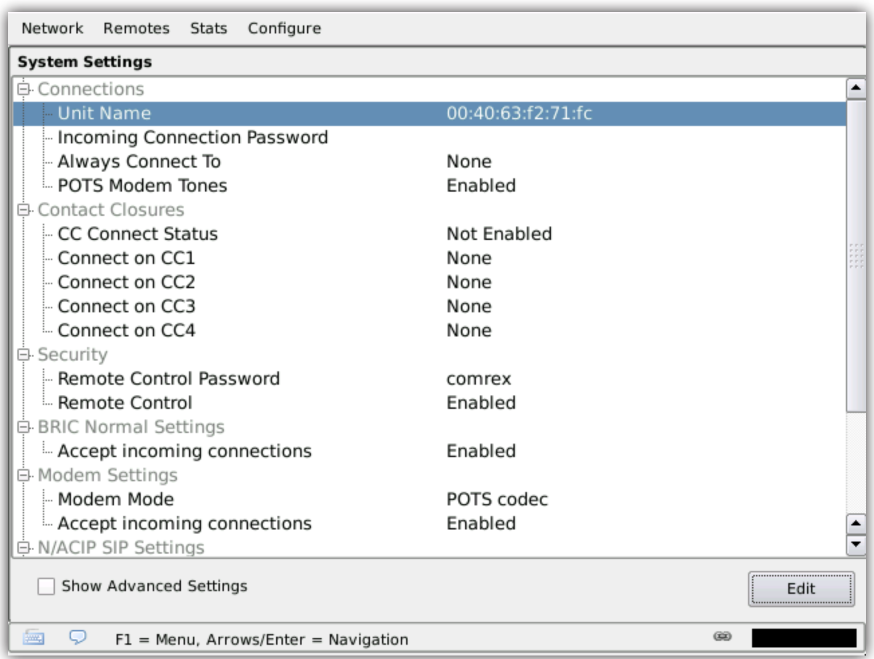


Figure 18 - System Settings Tab

User Interface

The **User Interface Tab** is shown below in Figure 19.

The F2 keyboard key can be user assigned to any of the most commonly used ACCESS functions. If you find you commonly use a function and are often scrolling through multiple menus to get there, simply assign the *F2 Key Behavior* to the proper function to create a shortcut.

The **Web Browser Home URL** setting allows you to change the default homepage for the ACCESS Web Browser.

ACCESS has many administrative features that are often unnecessary for the casual user. *Restricted User Mode* allows you to “hide” options that would confuse non-technical users, allowing them only to connect and disconnect calls, enable and disable available networks, and change the audio settings.

Restricted User Mode is enabled and disabled using the checkbox. It is not password protected, and can easily be disabled by any user.

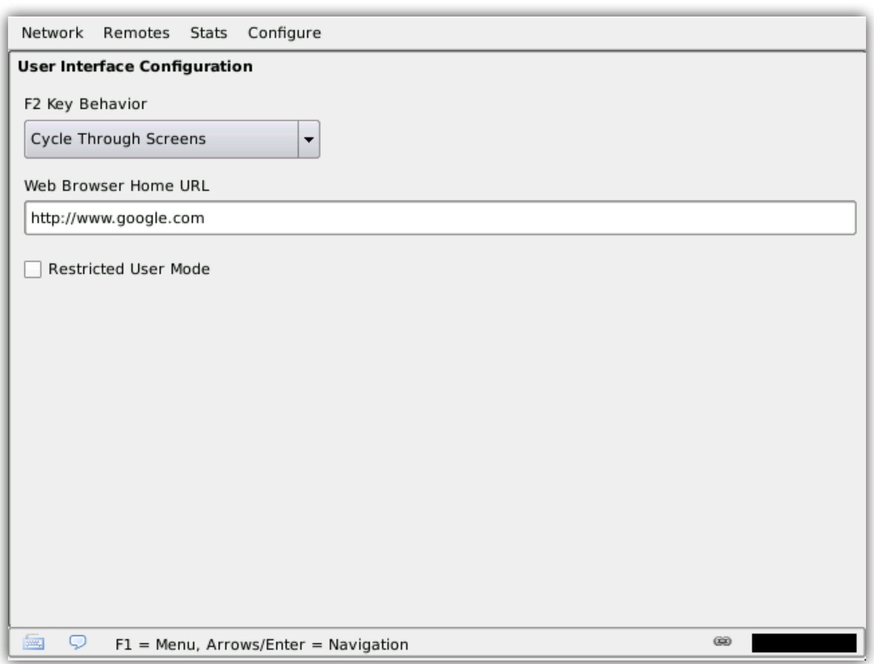


Figure 19 - User Interface Tab

Calibrate Touchscreen

ACCESS Rack supports connection of some VGA-style touch screen interfaces. Contact Comrex for tested models. In a mobile environment, this can allow a user-friendly interface without use of a PC or keyboard. USB-style touchscreens must be attached before booting the ACCESS Rack, and the user will be presented with a calibrations screen upon first connection. Once this calibration is done, the screen may be recalibrated by using this option. If no touchscreen is detected, this option is not available.

Reset Configuration

This option will restore your ACCESS software to factory default settings. WARNING: All settings, profiles, remotes and other changes will be lost in this procedure. This function is not reversible and should be used only as a last resort to restore factory settings.

SECTION 6 GAINING ACCESS TO ACCESS VIA THE WEB-BASED INTERFACE

ACCESS WEB-BASED INTERFACE

Once your IP settings are configured and ACCESS has cleanly booted on your LAN, it's time to take a look at the *ACCESS Web-based Interface*. This is done by pointing a web browser on your LAN to the ACCESS IP address. To do this, simply type the address into the URL bar of your browser. You will need Internet Explorer 6 or higher or Mozilla Firefox 1.0 or higher with Adobe Flash player. Opera 8.5 works well also. If you experience trouble connecting to ACCESS, be sure to check that your Adobe Flash player is current. Go to the following link to check and update your flash player.

http://helpx.adobe.com/flash-player/kb/find-version-flash-player.html

Once you are connected to ACCESS, a login screen will appear (see Figure 20). Key in any user name along with the default password (comrex, case sensitive) to get to the ***Main User Interface*** display. This display is optimized for full-screen mode (F11 on most browsers) on a 1024x768 display.

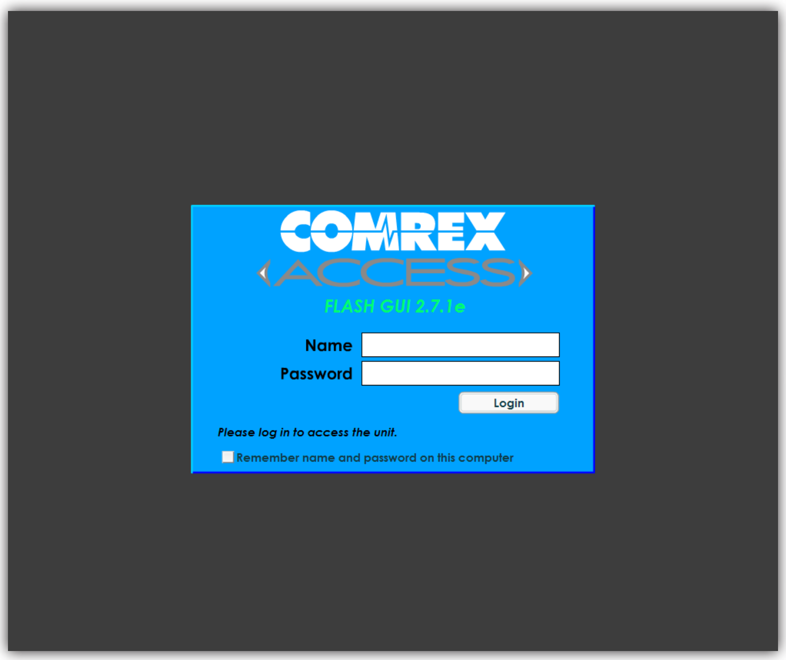


Figure 20 - Web-based Interface Login Screen

There are three main parts to the *ACCESS Web-based Interface* screen:

1) Main Audio Meter — The level meters are defaulted to off to conserve bandwidth and client CPU, but when these are enabled this top bar emulates the front panel of ACCESS.
2) Tabs — Use these tabs to control and obtain status of ACCESS. They are described in detail in the next four sections.
3) Chat Window — Allows for a chat utility between any users that are logged into that particular ACCESS web interface. In addition, when ACCESS is connected to a remote user, chat text will appear from any users logged into the remote web interface.
4) Registration Status — This window provides various network information and status, including Traversel Server status, (if licensed), SIP registration status, the units public IP address and NAT type.

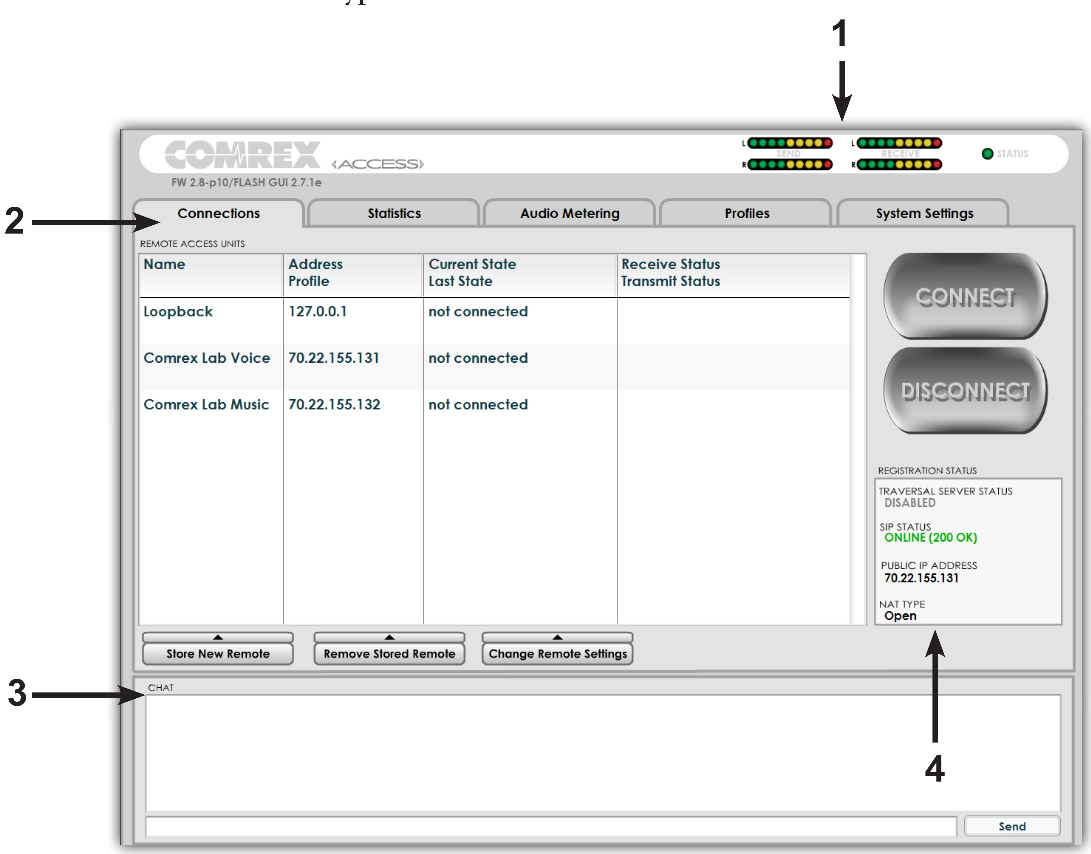


Figure 21 - Web-based Interface Screen

CONNECTIONS TAB

The following section describes how to enter "local" remotes into the product to dial them by IP address. If you plan on using the Switchboard Traversal Server, or take only incoming calls, this step may not be necessary. For more on Switchboard Traversal Server, see *SECTION 10*.

The **Connections Tab** is the default setting for the *Web-based Interface* (as shown in Figure 21). In this tab you can program and save the names and addresses of any remote units you connect to. This allows custom programming of policy parameters for each remote and allows point-and-click connect and disconnect. To add a remote ACCESS to the list, simply click **Store New Remote** in the lower section. An input box will appear allowing you to enter a user name (which can be anything) and the IP address of the unit. You will also need to choose a profile to use when connections to that remote are initiated. To get started, simply choose one of the default profiles provided (we'll show you how to build your own later). You may remove any stored value simply by highlighting and clicking **Remove Stored Remote**. Stored remote addresses are saved to system memory, where they will remain through power cycles.

The **Connection Tab** will also display **IP** and **Status** information of a remote ACCESS when it has initiated a connection to you. Their information will only appear while the connection is active.

By default, three users appear on the list. You may use any of these to test different encoder modes.

1) Loopback — Allows for connection between encoder and decoder in the same system.
2) Comrex Lab Voice — Allows testing back to the Comrex headquarters in Massachusetts, USA.
3) Comrex Lab Music — This additional user provides a music feed from the Comrex lab.

Statistics Tab

The **Channel Statistics** field (#1 in Figure 22) delivers information on the total number of bits entering or leaving the ACCESS (including multiple connections if applicable), IP, UDP and RTP packet headers and coded audio.

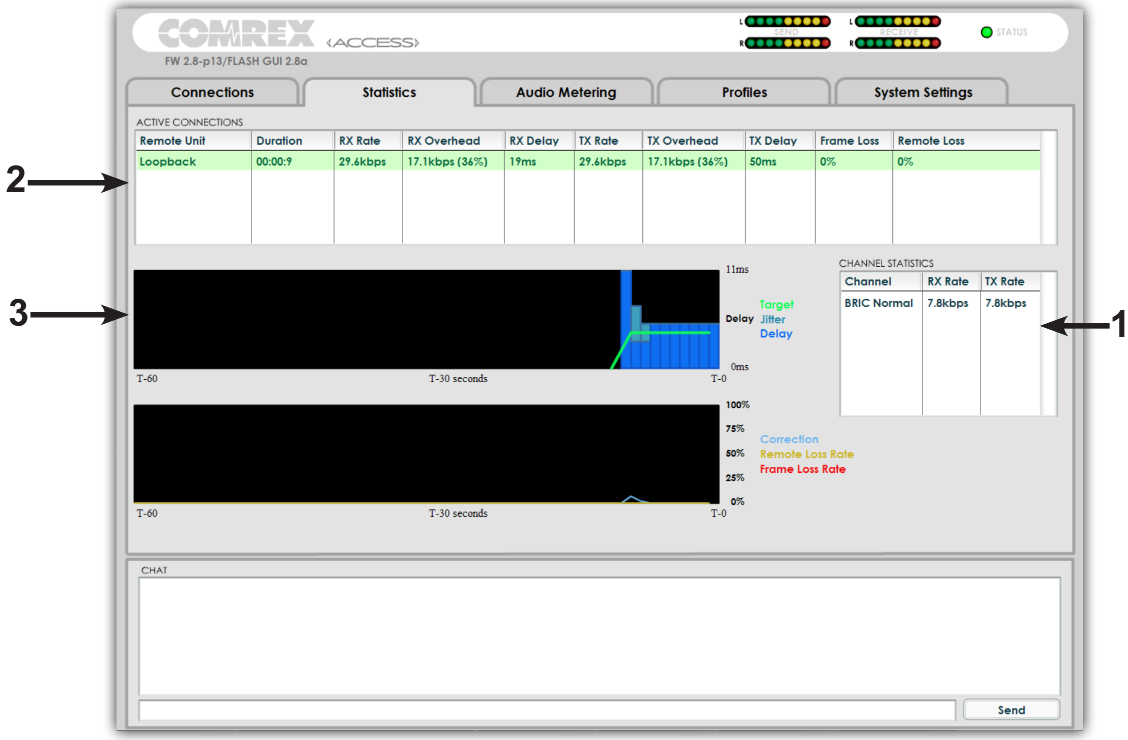


Figure 22 - Statistics Tab

The **Active Connections** box (#2 in Figure 22) breaks this information down further. Because ACCESS is capable of more than one simultaneous connection (in some modes), each connection is listed independently. **Receive Rate** and **Transmit Rate** are listed, along with an indication of how much overhead is required for the various IP headers on each packet. Frame Loss is also listed as an individual figure for lost and late packets. This table also includes an estimation of how much delay is attributed to each end of the link. This includes coding delay and buffering, but does not include any delay being caused by the network.

Graphical representations of **Jitter Buffer Manager** activity and **Frame Loss** are also displayed (#3 in Figure 22). The light blue area in the upper graph represents the jitter values over time. The work of the **Buffer Manager** is shown by the green line, which is the target buffer delay that the system is trying to achieve, based on measurements done over the jitter window.

The lower graph displays a real time and historical representation of frame loss. If the decoder does not receive packets in time, the chart will show a red line indicating percentage of lost packets over the one second interval.

AUDIO METERING TAB

The **Audio Metering Tab**, as shown in Figure 23, provides a representation of **Input** and **Output** audio levels in several formats. Each of these meters (including the top section meters, which are always visible) may be turned **On** and **Off** individually. All audio meters are defaulted to **Off** when ACCESS is first enabled. This is because transfer of audio level information consumes bandwidth on the local network, as well as CPU cycles on the client computer. Whenever ACCESS is connected to a data constrained network (e.g. wireless), it is strongly recommended that these meters be **Off**, especially if the *Web-based Interface* on the constrained network will also be accessed via the wireless network (e.g. from the studio end). The bandwidth requirements to drive the meters may affect performance of the audio codec.

The **Metering Quality** option (which is defaulted to low) adjusts how often the meters are updated—better networks can support higher quality settings. Refer to #1 in Figure 23.

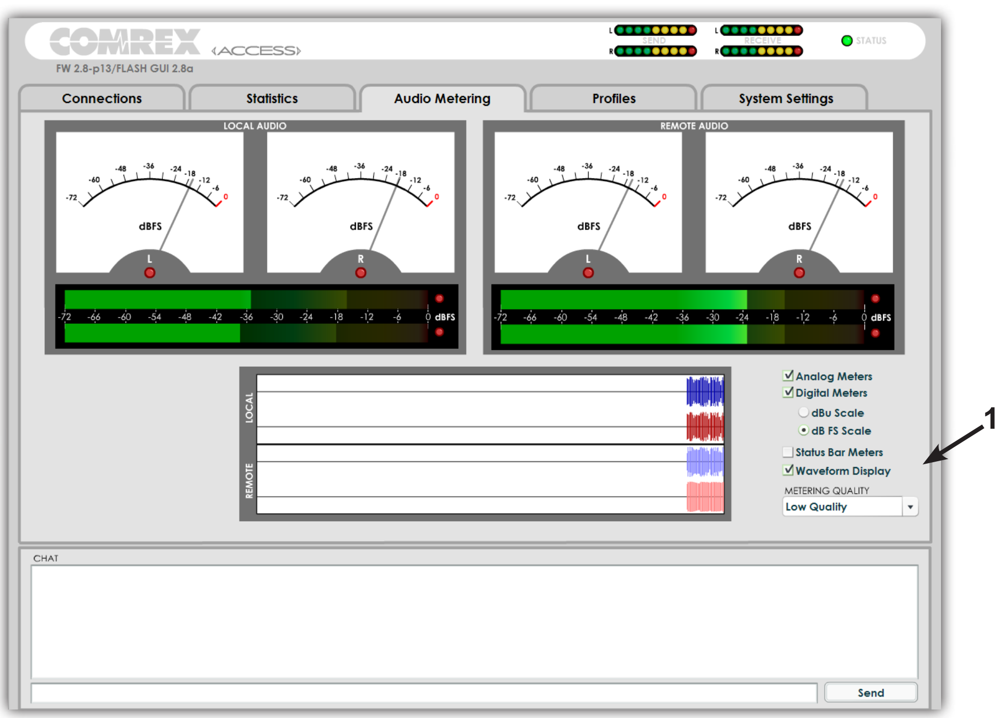


Figure 23 - Audio Metering Tab

Profiles Tab

ACCESS provides a powerful set of controls to determine how it connects. The **Profiles Tab** allows you to define one or more profiles to assign to outgoing remote connections. It's often not necessary to define any profiles, since ACCESS ships with a set of default profiles that cover most users. But this tab allows you to build custom profiles to allow for different encoders in each direction, special POTS coding modes, and special options for jitter buffer management. Keep in mind that these profiles are useful only for connections initiated from the local ACCESS. Incoming connections are defined by the ACCESS at the other end.

Profile creation is segmented into commonly used and advanced options. In order to simplify the interface, **Advanced Options** are normally hidden from the user.

Remember, building a profile doesn't change how any remotes are connected until that profile is assigned to a remote on the **Connections Tab**. Once a profile is defined, it will be available on the **Connections Tab** to be assigned to any defined connection.

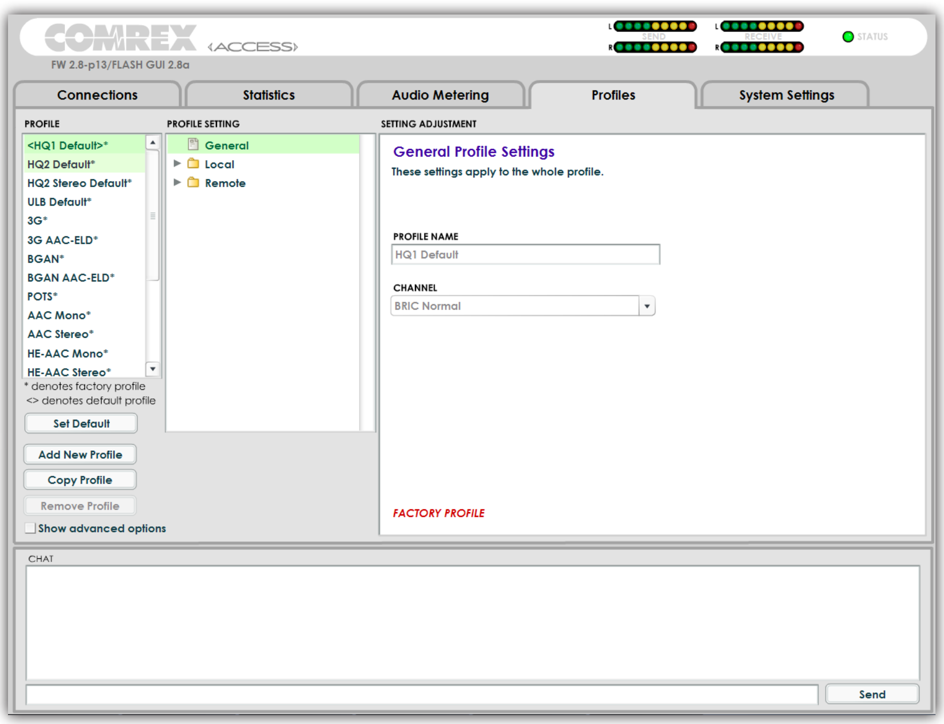


Figure 24 - Profiles Tab

BUILDING A PROFILE

We'll discuss the various profile options without the **Advanced Options** first, and move on to the advanced selections in the next section.

To build a new profile, select **Add New Profile** (#1 in Figure 25) and a new profile appears on the list labeled **New Profile**. Select it and you'll see the first set of options available in the **General Profile Settings** category (#2 in Figure 25). Here you can rename the profile to something that will help you remember it. Under the **Channel** category (#3 in Figure 25), you can select whether this is an IP connection (BRIC normal), a modem based connection (which uses the telephone line rather than the Ethernet jack) or IP Multicast (a method to deliver audio to multiple locations). *Note: It's important to define the channel of a profile before moving on to other options, since the choices in the subsequent sections will vary in this choice.* Make sure to press **Apply** in order to confirm your selection.

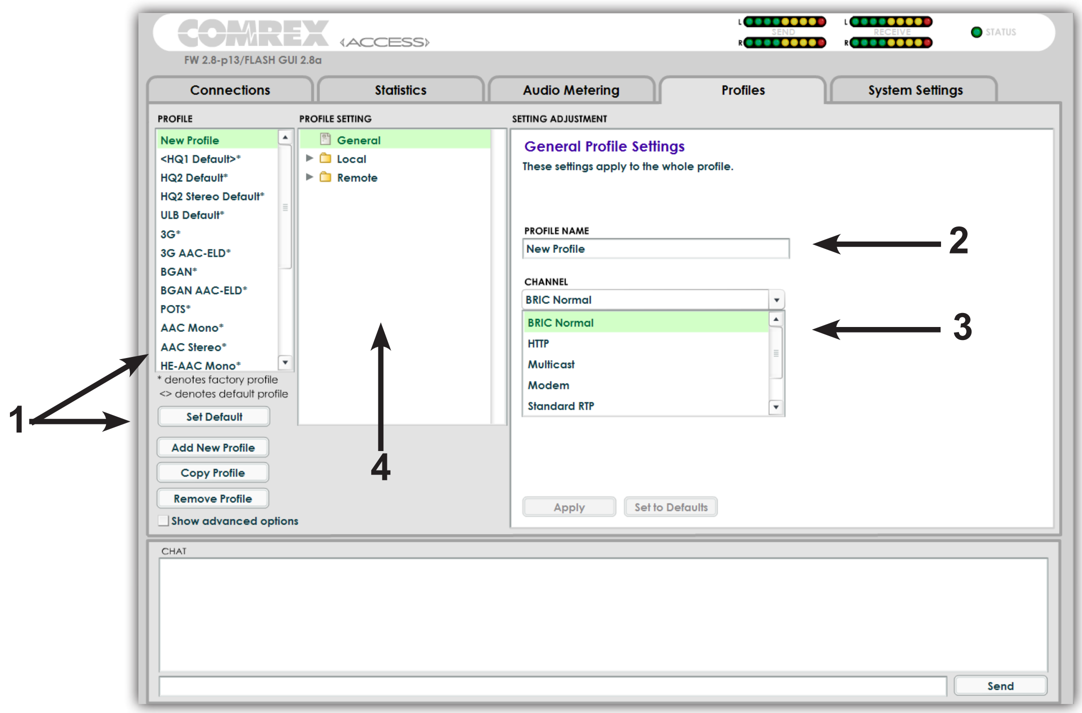


Figure 25 - Creating a New Profile

Local & Remote Settings

If you've chosen an IP-based channel (such as *BRIC Normal*) then you'll be presented with two categories of options: **Local** and **Remote**. You'll use the **Local Settings** to determine how your ACCESS behaves, and the **Remote Settings** will determine how the ACCESS on the far end behaves. Each category lists identical options, so we'll cover only the **Local Settings**:

Connection Timeout – Under normal circumstances, a connection will be terminated on one end and the other end will drop the connection in turn. But if a network failure occurs or a connection is ended abruptly (e.g. killing power to an ACCESS), the system will drop the connection after a pre-determined time. The default is 60 seconds, but this can be shortened or lengthened here. If an indefinite connection is required, see *Section 8 Operating ACCESS in a 24/7 Environment* for additional information.

Encoder – It's not necessary to define any decoder types when using ACCESS because they automatically adapt to the incoming stream. Using this menu, you can select the encoder used to send audio from this ACCESS (local) as well as the encoder used to send audio to this ACCESS (remote). The default value of the remote encoder is to follow the local encoder i.e. it will send exactly the same codec mode it receives. This is defined as **Follow Mode** in the remote encoder selection table. See *About the Algorithms* section for more info on selecting encoders.

Transmit On/Off – This option determines whether the selected encoder (local or remote) is actually sending any data. By default, all encoders are turned on, but there may be circumstances where one-way operation is desired (e.g. multi-streaming, as described in Section 12). Turning off the local encoder disables outgoing audio streaming, and disabling the remote encoder disables incoming audio streaming.

BRUTE Reliability Options

Two options are available to help transmissions that are suffering from poor network performance. There are encoder treatment options, so the are applied to the "local" encoder, the "remote" encoder, or both. BRUTE options require 2.7 or higher software on both ends of the link.

Congestion Avoidance – Enabling this option allows the encoder to dynamically change the number of frames/packet sent, thereby reducing total data requirements. In addition, in most encode modes, enabling congestion avoidance provides the system a license to step down to a lower encode data rate if desired. This will happen automatically and with no audio interruption. Step down congestion avoidance is not enabled in *ULB*, *HQ2*, or *Linear PCM* modes.

UDP Reliability – UDP, the Internet protocol used by BRIC Normal connections, does not have any inherent error correction capability. UDP reliability adds an intelligent algorithm that requests packet resends only when appropriate. UDP reliability can be useful on some wireless connections that have unsatisfactory performance due to packet loss.

POTS SETTINGS

For POTS connections, the choices are fewer:

Modem Mode – POTS Codec is the default setting and emulates the coding channel of previous Comrex POTS codecs like the Matrix, Vector and BlueBox products. ACCESS does not support compatibility with Hotline codecs. Stereo POTS allows connection between ACCESS users providing stereo audio over a dial-up connection. Compatible only with other ACCESS.

Connection Timeout – Under normal circumstances, a connection will be terminated on one end and the other end will drop the connection in turn. But if a network failure occurs or a connection is ended abruptly (e.g. killing power to an ACCESS), the system will drop the connection after a pre-determined time. The default is 60 seconds, but this can be shortened or lengthened here. If an indefinite connection is required, see *SECTION 8 OPERATING ACCESS IN A 24/7 ENVIRONMENT* for additional information.

SETTING UP ACCESS FOR USE ON POTS STEREO

In order to use *POTS Stereo Mode*, special configuration must be done on each end of the link. Once an ACCESS is set for incoming POTS stereo connections, normal mono POTS codec compatible calls can not be received until the settings are changed back.

Outgoing unit settings (usually the field unit) – The outgoing ACCESS will dial the phone call but a profile for the outgoing call that specifically uses *POTS Stereo Mode* must be built. This is done by creating a new profile in the **Profile Manager**. Select **Channel** under **Global Settings** and then **Modem** for the outgoing channel. Under **Local Settings** choose a **Modem Mode** of **Stereo POTS**.

Once the profile with these parameters is built, it can be named and assigned to any outgoing remote that uses a phone number (rather than an IP address) as its destination.

Additional profiles may be built utilizing the normal POTS codec modem mode, if desired. You can then build two remotes to the same phone number — one using your stereo profile and one using your legacy compatible POTS codec profile.

Incoming unit settings (usually the studio unit) – The incoming unit will receive the call from the field. In this case, the ACCESS must be configured to treat all incoming calls as *POTS Stereo Mode*. This is done in the **System Settings** section by selecting **Modem Mode** under **Modem Settings.** To receive stereo calls, this setting must read "Stereo POTS". To receive calls from older Comrex POTS codecs (or ACCESS configured to emulate them) the setting must be "POTS Codec".

ADVANCED PROFILE OPTIONS

The options available in the default mode should provide good performance for most users, but in some circumstances it may become important to fine tune some of the more obscure parameters that make ACCESS work. By clicking the **Advanced Options** box in the lower left of the **Profile Settings** screen, the following **Advanced Options** will be available:

ADVANCED CHANNEL

In addition to BRIC Normal and POTS, ACCESS provides the ability to set up several other channel types. The Advanced menu gives the option to use a different channel rather than the normal UDP/RTP created in BRIC Normal mode. Some explanation:

Internet IP packets come in two flavors: TCP and UDP. Most web browsing, email and other computer-based functions travel over the TCP protocol, which inherently assures retransmission if a packet is lost, and is therefore reliable. UDP is optimized for real-time applications, and does not offer any guarantee of packet delivery. Retransmission typically causes extra delay in an IP network, and ACCESS is optimized to conceal an occasional lost packet, so it makes more sense for ACCESS to use UDP for transmission under most circumstances. But there are occasions where a network will treat UDP packets poorly. Some examples are:

- Networks with high packet loss (rather than jitter)
- Networks with very high security firewalls
- Networks trying to discourage the use of VOIP functions

In these circumstances it makes more sense to enable a TCP channel. The result will usually be a more robust audio channel with a delay several magnitudes higher than an equivalent UDP channel. Channel overhead is also raised so you will utilize a higher network bandwidth.

In addition to TCP, there are several other advanced channel modes:

HTTP – ACCESS has the ability to act as a streaming server, delivering AAC and HE-AAC to compatible PC based media players. Normally in this mode, connections are requested on an incoming basis so no outgoing profile setup is required. But ACCESS also has the ability to initiate a stream to a Shoutcast-compatible server in order to distribute the stream to users. Only in this instance should a profile be set for HTTP.

Multicast – Should only be used to initiate IP Multicast connections (not for use on the Internet). See Section 13 for more on Multicast connections.

Standard RTP – This setting is used in the unusual scenario where the network is viable in only one direction. Standard RTP has the ability to send and receive streams without any status information being relayed between the codecs.

ADVANCED CHANNEL OPTIONS

When designating **Local** and **Remote** options for a normal BRIC or TCP channel, several new categories will appear. Some of them address the encoder and some address the decoder.

Most of the **Advanced Encoder** options alter the relationship between frames and packets. In this context, a frame is the smallest chunk of encoded audio that can be extracted from the encoder. For the lowest possible delay, this frame is wrapped into its own packet and sent into the network.

ADVANCED ENCODER OPTIONS

The following advanced option affect the Encoder:

Frames per Packet – Allows the encoder to wait for X number of frames to exist before sending a packet. This option differs from FEC because each frame is only sent once. Setting this value to a number higher than one can reduce network usage, at the expense of delay. This is because packet overhead bits like IP and UDP headers are sent less often.

Log Statistics – This function is used in factory diagnostics and should be left disabled unless instructed by Comrex support.

UDP Reliability Max Retransmissions – This parameter allows you to set an upper limit on how much additional bandwidth is utilized by the BRUTE UDP reliability layer. The default setting is 100, which allows the error

correction layer to use the same amount of bandwidth as the audio stream. As an example, if your audio stream is consuming 80 kb/s of network bandwidth, and UDP Max Retransmissions is set at 50%, up to 40kb/s additional network bandwidth may be used for error correction.

Nagle Algorithm – Nagle is applicable to TCP transmission only. When Nagle is enabled, encoder packets are sometimes buffered and concatenated into larger packets, depending on the network. It can be used to lower overhead on TCP networks, but adding delay.

ADVANCED DECODER OPTIONS

Advanced Decoder options have to do with how the jitter buffer manager performs. This is the algorithm that determines, based on network performance, how much delay to install in front of the decoder to achieve uninterrupted audio. It does this by creating a statistical analysis of the amount of jitter experienced over a fixed interval of time (the window) and making a judgment based on other parameters like the decoder's resiliency to errors. This is actually a very complex decision-making process involving many variables, and most of the time the default parameters should work well. The **Advanced Decoder** options are a means to override these defaults, and changing them should be done with care.

The following advanced options affect the **Decoder**:

Retransmit Squelch – These options are used to determine how the buffer manager reacts to typical data dropouts like those seen on wireless networks. Some explanation:

Many wireless networks have their own layer of data protection riding on top of any other data layer, providing packet retransmissions in the event of signal fade. The symptom from the network standpoint is that data will come to a stop for some period of time while the signal is faded, and the network will buffer all packets during this time. Once the wireless link is restored, all the buffered packets will appear to the decoder as if they were simply very late. In essence, the protection layer will "fight" the buffer manager. The effect will be that the buffer manager will expand the buffer, increasing delay dramatically without any benefit.

The **Retransmit Squelch** allows the decoder to detect these events and avoid having the buffer manager react. The squelch has several user adjustable parameters with good default settings. These should normally be left where they are, but there may be unusual circumstances where they should be changed.

Retransmit Squelch Trigger – Determines the amount of time the decoder must experience 100% packet loss before the **Retransmit Squelch** function is triggered. Default is one second.

Retransmit Squelch Max – The longest period of data loss during which the squelch function is active — the default is two seconds. During the squelch period, the buffer manager ignored the relative jitter experienced and does not adjust buffer size to compensate.

Jitter Window – This parameter defines the amount of time (in minutes) that historical network performance is analyzed in order to make the rest of the calculations. As an example, if the **Jitter Window** is set to the default of five minutes, and if a dramatic network event happens and the buffer manager reacts (perhaps by increasing the buffer), the event will be included in the manager's calculations for the next five minutes. If the network experiences improved performance over this period, the manager may choose to wind the buffer back down after the five minutes has passed.

Loss Cushion – Packets may arrive at the decoder displaying a range of statistical properties. They may arrive in reasonably good timing and in order, or half may arrive quickly with the other half delayed significantly. In some cases, most of the packets arrive in a timely manner, but a small percentage of them may be extremely late. In this case, it's usually preferable to allow these late packets to be left out, and keep the delay lower. The decoder error concealment does a very good job of hiding these losses. The **Loss Cushion** parameter instructs the buffer manager to ignore a certain percentage of late packets in its calculation. The default value is 5%. Applications that are not at all delay sensitive may wish to reduce this value to zero, while extremely delay sensitive applications may prefer to have this closer to 25%.

Delay Cushion – The jitter buffer manager usually works very hard to keep absolute delay to a minimum. Some applications are not delay sensitive and would rather not have the manager working that hard. The **Delay Cushion** setting is a way to instruct the manager not to attempt to drive the delay below a certain value. E.g. if the delay cushion is set to 500mS, this amount of fixed delay will be added to the buffer. If the jitter manager needs to increase the buffer it will do so, but will not fall below the ½ second level.

Delay Limit – The inverse of the **Delay Cushion**, this parameter instructs the manager not to wind the buffer out beyond a certain delay value, regardless of how many packets are lost. This is useful in applications where staying below a certain delay figure is essential, but use of the delay limit can result in very poor performance if the network jitter dramatically exceeds the limit.

Fixed Delay – This option simply sets the **Delay Cushion** and **Delay Limit** at a similar value, so that the delay buffer is defined to the chosen value and will not increase or decrease significantly.

Buffer Management On/Off – This option is available only as a troubleshooting tool. Turning the manager off will result in eventual failure, since the manager is required to compensate for clock skew between the encoder and decoder.

System Settings Tab

The **System Settings Tab** defines parameters that are not specific to a particular remote connection. Examples are how incoming (POTS and IP) calls are handled, global modem settings, and how the contact closures are assigned. The **System Settings Tab** is shown in Figure 26a.

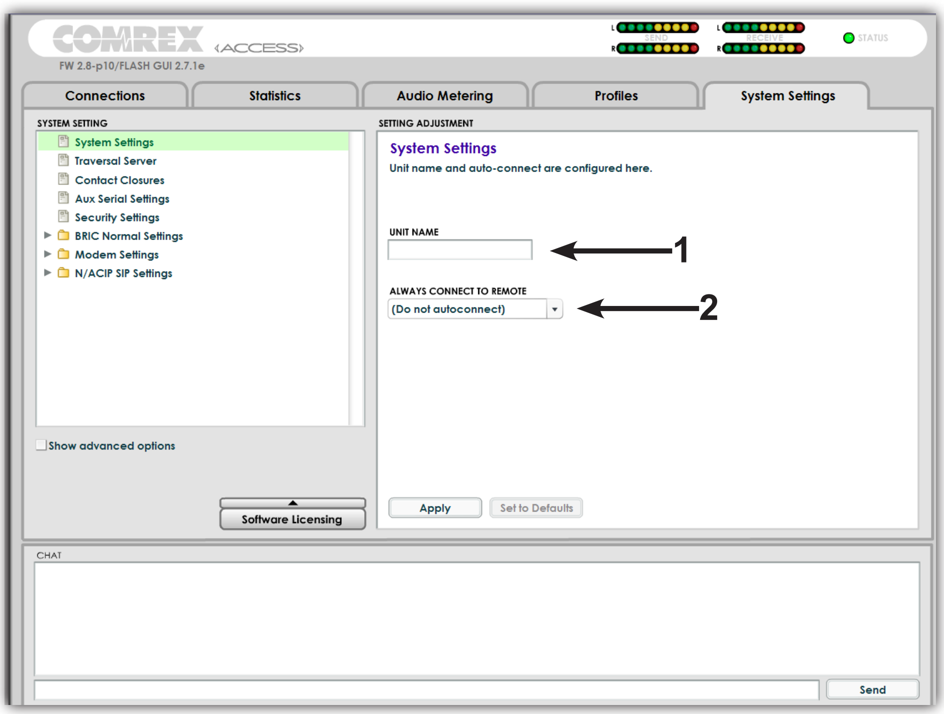


Figure 26a - System Settings Tab

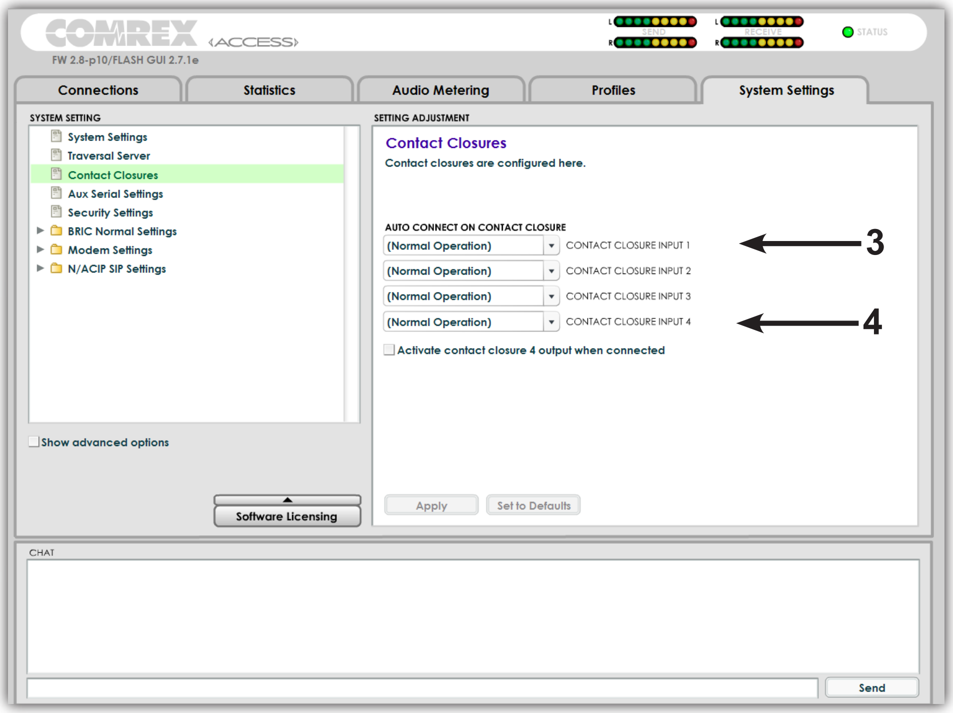


Figure 26b - System Settings Tab

The **Systems Settings Tab** has several categories: **System Settings**, **Traversal Server, Contact Closures**, **Aux Serial Settings**, **Security Settings**, **BRIC Normal Settings**, **Modem Settings** and **N/ACIP SIP Settings**. As with the **Profile Tab**, basic options are shown by default. Less used options are hidden until the **Show Advanced Options** box is clicked.

Unit Name – Users are encouraged to name their codecs here. The default name of a codec is the unique MAC address of the Ethernet port. By changing this to something familiar and unique (e.g. roving reporter, weather guy, etc) this name is reflected in several places:

1) In the browser used to show the remote control page
2) In Comrex provided utility software such as **Remote Control** and **Device Manager**
3) In Switchboard TS Buddy lists (See Traversal Server Section)

Always Connect to Remote – #2 in Figure 26a shows the system **Auto Connect** options. Remote connections must be created in the **Connections Tab** before they can be assigned to any of these functions. One field is available to designate a remote for always on operation. This is useful in “nailed up” environments, where a signal is required across the link 24 hours a day. To assign an always on remote, simply pull down the menu and select which remote to designate as **Always On**. A connection will be made and sustained to the chosen remote.

CONTACT CLOSURES

The Auto connect on contact closure fields (#3 in Figure 26b) define auto connect rules for remotes to be triggered by the four external triggers available on the rear panel of the ACCESS. *Note: These inputs are shared with the end-to-end contact closure signals, so if a remote is designated as **Auto Connect** on a closure, that closure signal is sacrificed in the direction from this ACCESS.*

To assign a remote connection to a contact closure, simply pull down the menu box next to the desired closure and select the proper remote. A connection attempt will be made whenever the contact is triggered, and will disconnect whenever the contact is released.

CC Connect Status – This setting (#4 in Figure 26b) alters the performance of output contact closure #4. Under normal circumstances the signal indicates a trigger of the corresponding contact closure input on the far end of the connection. If this box is selected, that function is no longer available, and the signal follows the ACCESS front panel **Ready** light. This signal will be valid (closed) when a valid connection is present, and invalid (open) when no connection is present.

AUX SERIAL SETTINGS

This allows you to set the parameters of the auxiliary serial data port provided on the ACCESS. This port is always active during an IP connection and allows serial data transfer along the same path used for the audio data. It does not remove any audio data; the serial data is added to the packets and bandwidth is increased to support the additional data. For this reason heavy use of serial data can affect overall codec performance. Settings are available for Baud Rate, Data Bits, Stop Bits, Flow Control and Parity. Most users will leave the defaults of 9600, 8, 1, No Flow Control and No Parity.

SECURITY SETTINGS

Connection Password – Allows you to define a password that must be attached to all incoming connections before they are accepted. Units placing outgoing connections to you must know this password and apply it to their outgoing stream. Leaving the field blank will disable this function.

GUI Password – Allows you to define a password for the web page login screen and firmware updater. The default password is comrex (lower case). You can disable the remote control and firmware updating functionality completely by disabling the **Remote Control** option.

Enable Remote SSH Access – Provides the ability for Comrex support to connect to this unit using the SSH protocol in order to troubleshoot. We recommend leaving this option enabled, since SSH access requires a key value that is not disclosed by Comrex, generic SSH requests are rejected.

BRIC Normal Settings

Accept Incoming Connections – This determines if this ACCESS is to used for incoming normal IP connections. If this function is not enabled ACCESS will only support outgoing calls using *BRIC Normal Mode*.

Modem Settings

Modem Mode – This setting determines which of the two POTS modes is to be used for incoming calls. One limitation of ACCESS' *POTS Codec Modes* is that both ends must be set correctly for POTS codec calls to work. The default setting is **POTS codec**, which causes ACCESS to answer incoming POTS calls that are compatible with ACCESS, Matrix, BlueBox and Vector codecs (but not Hotline). More information on may be found in *Section 9 POTS Codec Connections*. The other option is **Stereo POTS**. *Stereo POTS Mode* provides a stereo audio signal over a single dial-up phone connection. It utilizes a POTS-optimized version of the *HQ2* algorithm. This mode utilizes intensity stereo coding, so channels may not be used to send uncorrelated audio material i.e. they must be left and right channels of a stereo feed.

Again, ACCESS does not have the ability to adapt between the two types of POTS calls it supports. The proper mode must be selected before an incoming call of that type is received.

Accept Incoming Connections – POTS calls must be answered automatically on ACCESS. If this option is disabled, no POTS calls will be answered and only outgoing POTS connections can be made.

N/ACIP SIP Settings

For information on the N/ACIP SIP Settings, please see *Section 16 - Making N/ACIP SIP Compatible Connections.*

Advanced System Settings

When the **Advanced System Settings** box is checked, a few additional options are enabled.

BRIC Normal Settings

IP Port – This option allows you to define the incoming UDP port: the number to be used for incoming IP connections. The default is 9000. Note that since most ACCESS codecs attempt a connection on this port number, changing it can mean ACCESS in the field must dial specifically to your new port number in order to connect. An outgoing call must be made to a specific port number in the form of IP_ADDRESS:PORT e.g. dialing port 5004 on the Comrex test line is formatted 70.22.155.131:5004

Modem Settings

Ring Count – For Incoming POTS calls, this setting determines how many rings to allow before answering.

Max Modem Rate / **Min Modem Rate** – These settings constrain the modem and instruct it not to connect higher than the **Max** or lower than the **Min**. This is valid for incoming and outgoing POTS calls.

Extra Modem Init – This option will allow the entry of special initialization strings to be sent to the internal modem before a call is placed. These strings can change things like country of operation, dial tone and ring cadence frequencies, and other phone-line based parameters.

Standard RTP Settings

These settings offer several modes that allow compatibility with specific IP coding devices. For complete details please review the *IP Compatibility* appendix of this manual.

N/ACIP SIP Settings

For information on the N/ACIP SIP Settings, please see *Section 16 - Making N/ACIP SIP Compatible Connections.*

RTP IP Port – Port used for audio transfer during N/ACIP SIP mode. Since this port info is transferred during the negotiation process, it can be changed without breaking compatibility. Note that RTSP data is always sent and received on the port one address higher than this.

Public IP Override – Enable this in an environment where ports have been forwarded through a router to the ACCESS, and a N/ACIP SIP connection is desired. The SIP protocol is assuming no ports are forwarded, and may have trouble connecting without this function enabled.

TCP Settings

ACCESS performs best when using UDP for connections but there are some rare circumstances when the system may need to be switched over to TCP operation. This advanced option defines how incoming TCP calls are handled.

Outgoing calls are defined as TCP when their profile is configured. ACCESS normally listens for incoming calls on both TCP and UDP ports, and chooses the first to arrive. If a TCP call is detected, ACCESS will attempt to use the same TCP link to transmit in the reverse direction.

Accept Incoming Connections – Allows you to turn *TCP Auto Answer* on and off. Disabling this function means only outgoing TCP calls call be established.

IP Port – You have the option of setting the incoming TCP port number, which can be different than the UDP port number. Note warnings given above about changing port numbers — calls with mismatched port numbers will fail.

SECTION 7 MAKING CONNECTIONS USING THE WEB-BASED INTERFACE

The following section describes how to enter "local" remotes into the product to dial them by IP address. If you plan on using the Switchboard Traversal Server, or take only incoming calls, this step may not be necessary. For more on Switchboard Traversal Server, see *SECTION 10*.

CREATING A REMOTE CONNECTION

So now it's time to make a connection on ACCESS. We will assume that the proper network and audio connections have been made. Before you can establish an outgoing connection on ACCESS, you must enter the info about remote connection into the **Connections Tab**. This acts like a phone book, saving the names and numbers of everyone to whom you connect.

As shown in Figure 27, ACCESS comes pre-programmed with three connections. Loopback is chosen when you wish to test ACCESS by connecting the local encoder and decoder together. The other two entries are connections to Comrex in Massachusetts, and these may be used for your testing (when they're not busy with other users). We maintain two CD players on these ACCESS, feeding voice and music audio respectively.

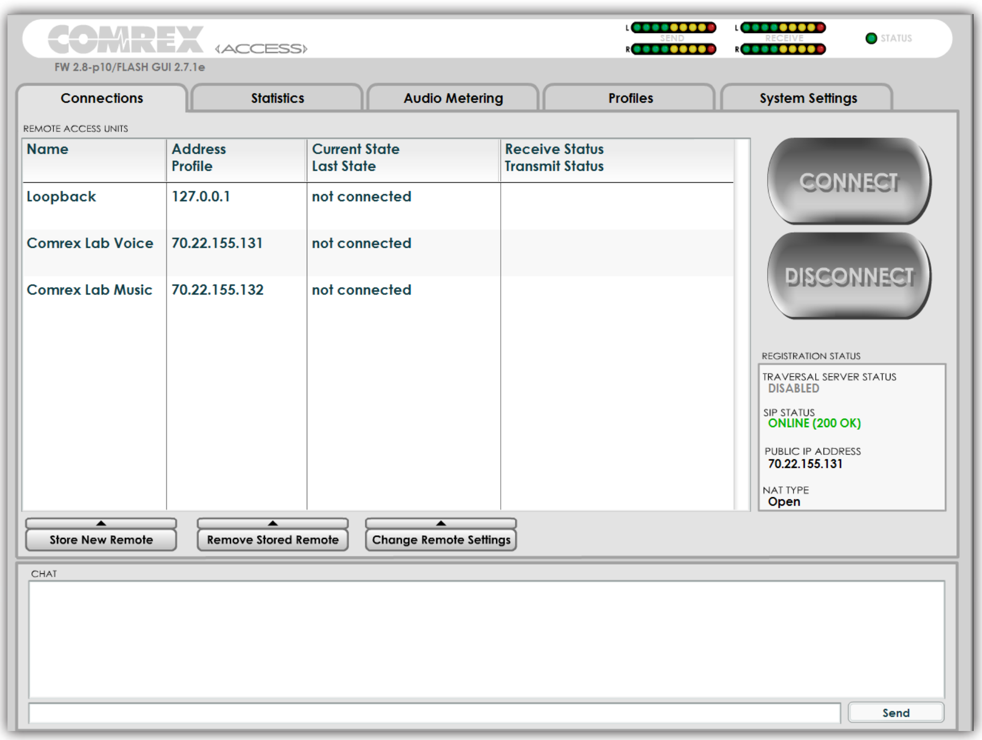


Figure 27 - Connections Tab

To create your own outgoing connection, click **Store New Remote** (#1 in Figure 28) to get the entry pop-up. Choose a name for the remote (e.g. WXYZ) followed by the IP address or phone number of the remote. The next field is optional. If the remote has password filtering enabled for incoming calls, you will need to enter that password into the next field (case sensitive) in order to make a connection to it (see *Password Filtering* in the next section for further information). If no password is required, leave this blank

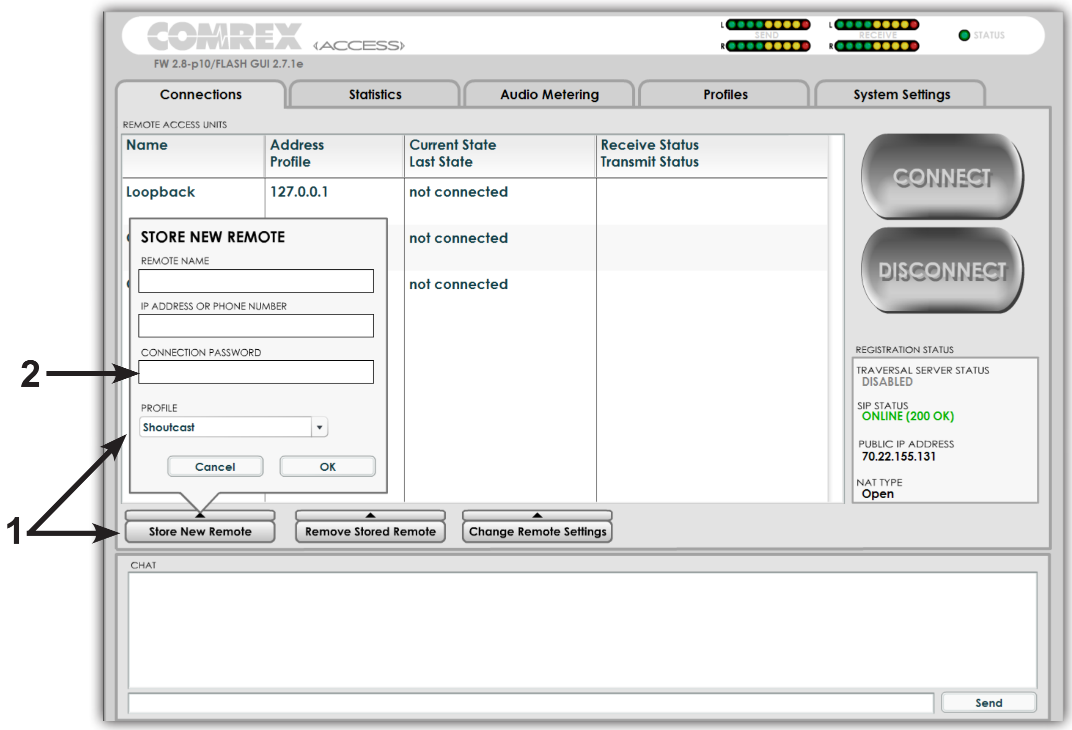


Figure 28 - Store New Remote in the Connections Tab

Finally, you will need to choose a profile to use when making these connections. ACCESS includes several common default profiles to choose from, each of which enable a simple full-duplex link using one of the available algorithms. If you wish for a more complex feature set when making this connection, you will need to click over to the **Profile Tab** and set up a specific profile using your custom parameters. Custom options can include one-way transmission, different encoders in each direction, specialized packet arrangement, etc. Once defined on the **Profile Tab**, the new profiles will be available in the **Profile** select window and they can be assigned to a remote connection.

Once your remote connection entry is correct, it's simply a matter of pointing and clicking to connect and disconnect a remote. When a connection is attempted, the **Current State** value in the connection table will change to reflect the progress of the connection. If the connection fails, the reason for failure will be shown in the **Last State** category. If it succeeds, the encoder and decoder mode will be reflected in the **Transmit** and **Receive Status** columns.

DISCONNECTING

Disconnecting is just as simple — Highlight the desired connection and click **Disconnect** to end the connection.

ADVANCED CONNECTION OPTIONS

PASSWORD FILTERING

The **Connection Password** function can be used to filter incoming BRIC IP connections (but not POTS calls). Using this function, attempted incoming connections will be rejected if they do not know the proper case-sensitive password. For outgoing connections, the password is entered when the remote connection is created on the **Store New Remote** menu (#2 in Figure 28). For incoming connections, the password is set on the **System Settings Tab** (#1 in Figure 29). There isn't any way to retrieve a forgotten password; it must simply be changed in each ACCESS.

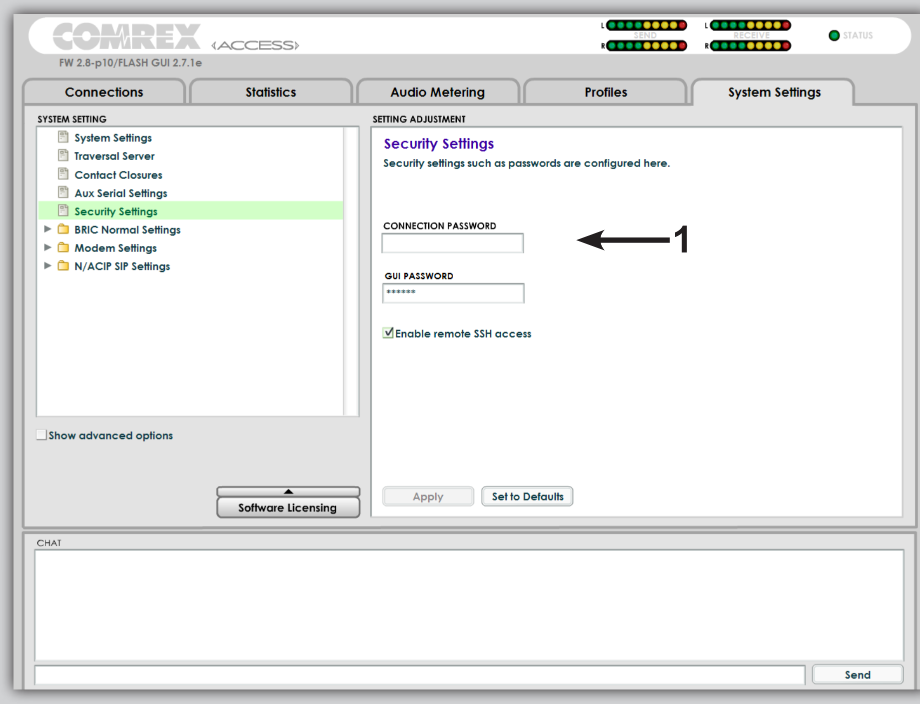


Figure 29 - Connections Password in the Settings Tab

Connecting to a Specific Port

BRIC IP connections (and all IP traffic) use a concept known as ports to differentiate between different applications on the same computer. A port is simply a number contained in the IP header, but it can be treated as a physical opening in and out of your computer. Most firewalls function by opening the network to traffic with only specific port numbers.

Each IP connection has a source and destination port. Under most circumstances, the source port is unimportant, but the destination port can be key. Certain incoming ports can be firewalled to outside traffic, and in the case of several ACCESS behind a router (sharing a single public IP address), the only way for them all to take incoming calls is to assign different incoming ports to each device.

To transfer audio, ACCESS uses a default source and destination port of 9000. If this is changed, both the outgoing and incoming ACCESS must be made aware of the change.

Changing the port for incoming connections is done on the **System Settings Tab**. Because this can really mess things up if not done properly, the function is hidden in the **Advanced Options** of this tab (as shown in Figure 30). Access the **Advanced Options** by clicking the **Show Advanced Options** box in the lower left corner of the **System Settings Tab**.

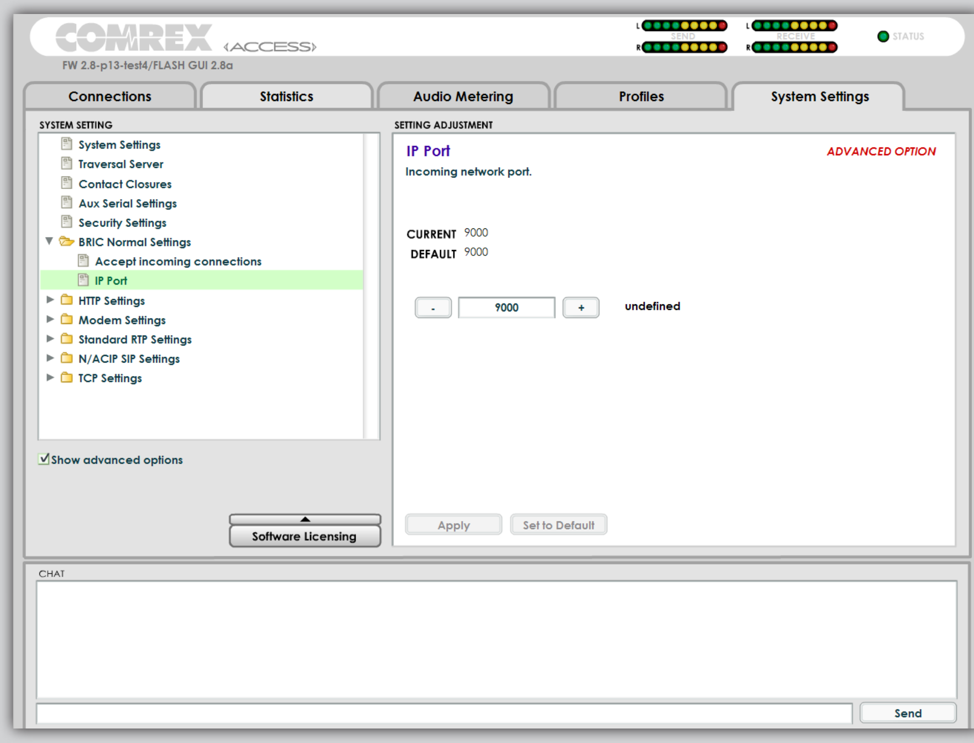


Figure 30 - Changing the UDP Port for Incoming Connections

To change the destination port of an outgoing call, you must add the port number to the IP address in the following format:

IP_address:port_num

For example, to initiate a connection to the Comrex test line at port number 5004, enter the following into the IP address field:

70.22.155.131:5004

Note: The call will fail unless the ACCESS on the far end is set to receive data on that port.

Backing up a Connection

ACCESS features an ability to have an automatic backup to IP remote connections. The backup may be either another IP connection, or a POTS phone number. Automatic backup works as follows:

If an IP connection fails, ACCESS will sense this and wait the amount of time designated in the **Local Timeout** parameter in the profile assigned to the primary connection. If the connection is restored in that amount of time, no backup will occur.

If the timeout period passes without restoration of the primary connection, ACCESS will automatically establish a connection (POTS or IP) to the designated backup connection. It will maintain that connection until manually disconnected.

Backup connections are enabled and selected on the **Change Remote Settings** option on the **Connection Tab** (shown as #1 Figure 31).

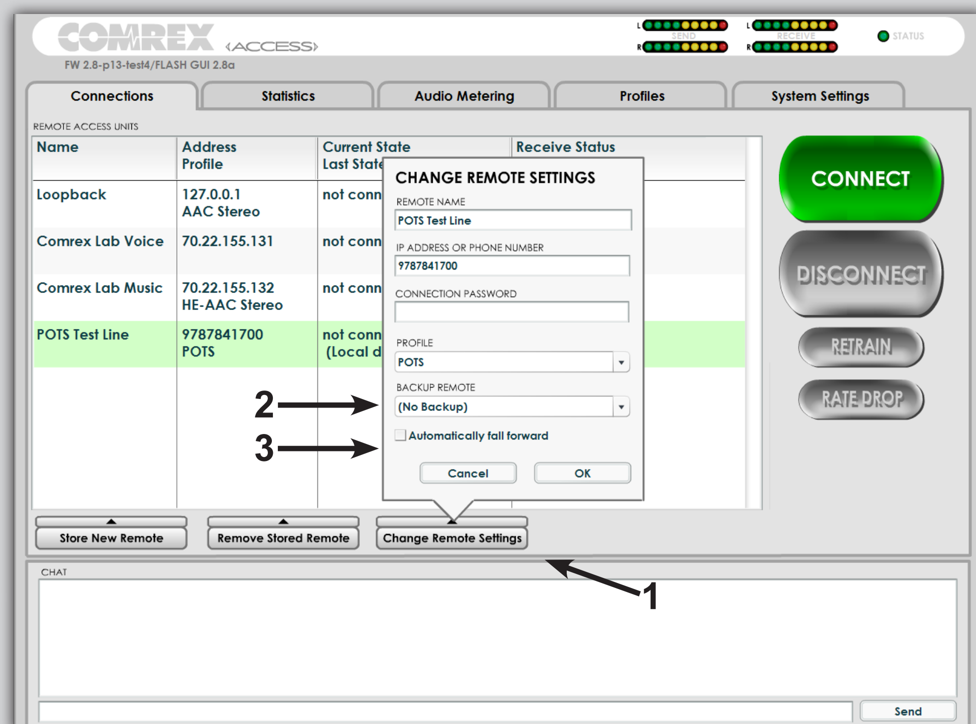


Figure 31 - Backup/Fall Forward Functions in the Connections Tab

FALL FORWARD FUNCTION

To enable an automatic backup, both the primary and secondary remote connections must first be defined and assigned profiles. Next, select the primary remote and click **Change Remote Settings**. On this pop-up, choose the pull-down menu labeled **Backup Remote** (#2 in Figure 31) and select the backup for this primary connection.

BACKUP/FALL FORWARD LIMITATIONS

By selecting the **Automatically Fall Forward** function in this pop-up (#3 Figure 31), you will enable ACCESS to monitor the primary IP connection while the backup is active. If the primary is restored and is detected to be valid for the timeout period, the backup will be disconnected and operation will revert to the primary.

The **Backup/Fall Forward** functions have the following limitations:

1) Only IP connections can be designated as primary — IP or POTS connections can be backups.
2) **Fall Forward** does not work when the POTS backup is the same physical ACCESS as the primary IP. This is because ACCESS receiving incoming POTS calls cannot restore IP connections.

Section 8 Operating ACCESS in a 24/7 Environment

ACCESS can be easily set up for “always on” operation. It will be helpful to describe a little bit about the ACCESS data transfer protocol before describing how to set the system up.

In *BRIC Normal* mode, the default mode of operation, ACCESS transfers all its audio data via the UDP protocol. This is in contrast to most web-based connections like browsing and e-mail, which use the TCP protocol. UDP, unlike TCP, is not “connection oriented” i.e. no virtual connection actually exists in this protocol layer between the devices. In UDP, the transmitter simply launches packets into the network with the correct address, hoping the network will make its best effort to deliver the packets in a timely fashion. If a packet is delayed or lost, no error message is sent and no packets are retransmitted. It is up to the receiver to cover up any lost data, if it can. This allows the Internet to deliver packets with the smallest amount of overhead and delay.

Since there is no intelligent connection built between the codecs, there isn’t actually any connection to break in the event of network failure. The encoder simply launches packets into the network, regardless of whether they arrive or not. If the network fails and is later restored, the packets stream will be restored to the decoder.

For most applications like remote broadcasting, it’s useful to simulate a connection-oriented stream, so ACCESS uses a low-bandwidth sub channel to deliver information back to the encoder about overall connection status. It does this in its “application layer”, rather than the “transport layer” where UDP exists. By default, it monitors the health of a connection and, if no data is detected as received by the decoder for 60 seconds (this is a user adjustable timeout) it “tears down” this connection and goes back to idle state. This can give an indication to the user that the network has failed and it’s time to look at the problem.

The good thing about having the connection protocol in the application layer is that its use is optional. For 24/7 operation, there’s no advantage to having the connection end if no data is received for a timeout interval. So to set ACCESS for 24/7 operation, several parameters are changed:

1) The timeout value is set to infinity—the connection will never be torn down regardless of data status.
2) ACCESS is configured to re-establish the connection in the event of a power-up.
3) The local **Disconnect** control is disabled. The **Disconnect** function on the receiving side is still enabled, but will result in an immediate reconnection by the initiating side.

SETTING ACCESS FOR 24/7 OPERATION

As shown in Figure 32, using the *Web-based Interface*, 24/7 operation is initiated in the **System Settings Tab** (using the *Console Connection Interface*, this is found in the **Connections** section of the **System Settings** menu.). The field labeled **Always Connect To Remote** offers a pull-down menu of all available connections. Setting this value to one of your pre-defined connections results in configuring the unit for 24/7 operation to that remote. No configuration is necessary on the remote side.

ACCESS has another option for persistent connections. When building a remote entry a field is available for backup options; one of those options is *Keep Retrying This Remote* mode. In a similar fashion, using this mode will disable the connection timeout setting and keep a persistent connection. The difference is that the **Disconnect** function still works and the connection will not be reinitiated on a power-up. This mode is meant for users who are making temporary connections, but do not want the system to time out and disconnect in the event of network failure.

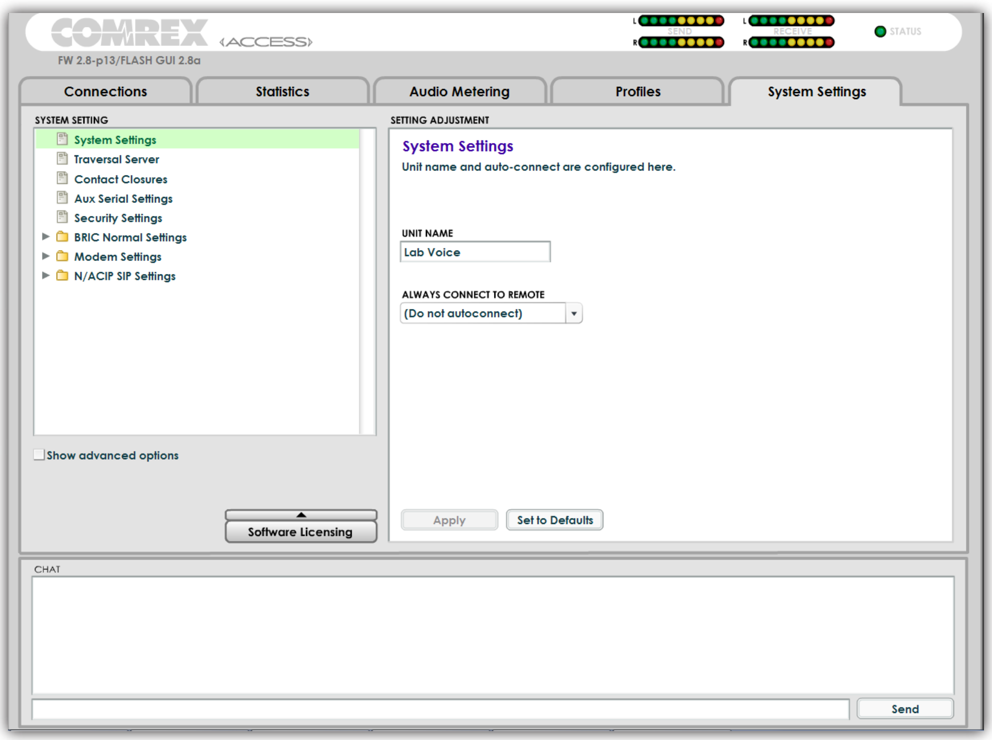


Figure 32 - 24/7 Operation in the Connections Tab

SECTION 9 POTS (PLAIN OLD TELEPHONE SERVICE) CODEC CONNECTIONS

ACCESS is capable of connections over modem links. This mode emulates the function of Comrex POTS codecs, which have been used for years to deliver high quality audio over normal, dial-up telephone lines. This mode provides for a point-to-point connection between the codecs i.e. no internet access is used, and the call is placed directly from one ACCESS (or legacy codec) to the other.

In the current firmware, ACCESS is capable of connecting over dial-up phone lines to:

ACCESS Codecs
Comrex Matrix Codecs
Comrex BlueBox Codecs
Comrex Vector Codecs

Note: Backward compatibility to Hotline codecs is not supported.

POTS Codec Set-up for ACCESS Compatibility

The legacy codecs (Matrix, Vector or BlueBox) must be configured for operation in *Music Mode*, which will allow full-fidelity (up to 15 KHz) connections. *Voice Mode* is not supported by ACCESS. Contact closures and ancillary data supported by legacy codecs are not supported by ACCESS.

ACCESS requires that outgoing POTS connections be defined on the **Connections Tab**. When defining any outgoing connection, a profile must be assigned to it. For POTS Codec compatible connections, the factory default **POTS Profile** should work best. *Note: When creating a profile, you must designate the modem mode as **POTS Codec** rather than **POTS Stereo** in order to be compatible with legacy devices. This is shown in Figure 33.*

Using ACCESS with POTS

To use ACCESS on POTS, a normal, analog telephone line must be connected to the rear panel telephone line RJ-11 connector. If possible, try to obtain a true telephone company grade line, rather than an extension from your digital phone system. Under no circumstances should the raw extension from a digital phone system be attached to this port—you will likely damage ACCESS, your phone system, or both.

To initiate calls from ACCESS, simply create a remote connection with a telephone number as an address, rather than an IP address, in the **Connections Tab**. You must designate a POTS-based profile for this remote.

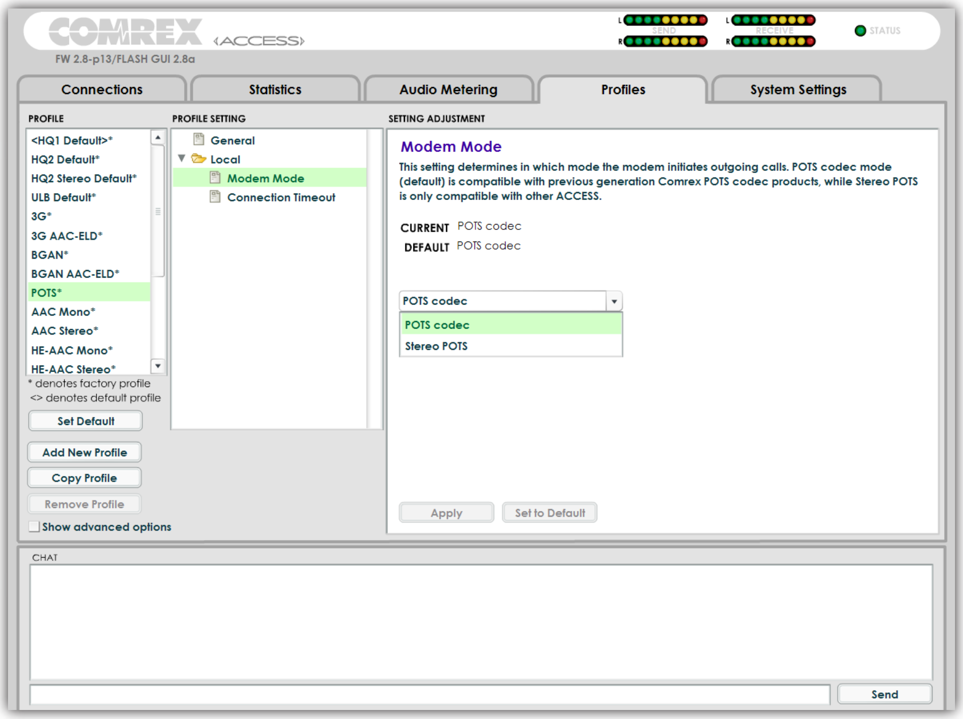


Figure 33 - POTS Codec vs. POTS Stereo Mode in the Profiles Tab

SETTING UP ACCESS FOR USE ON POTS STEREO

In order to use *POTS Stereo Mode*, special configuration must be done on each end of the link. Once an ACCESS is set for incoming POTS stereo connections, normal mono POTS codec compatible calls can not be received until the settings are changed back.

Outgoing unit settings (usually the field unit) – The outgoing ACCESS will dial the phone call but a profile for the outgoing call that specifically uses *POTS Stereo Mode* must be built. This is done by creating a new profile in the **Profile Manager**. Select **Channel** under **Global Settings** and then **Modem** for the outgoing channel. Under **Local Settings** choose a **Modem Mode** of **Stereo POTS**.

Once the profile with these parameters is built, it can be named and assigned to any outgoing remote that uses a phone number (rather than an IP address) as its destination.

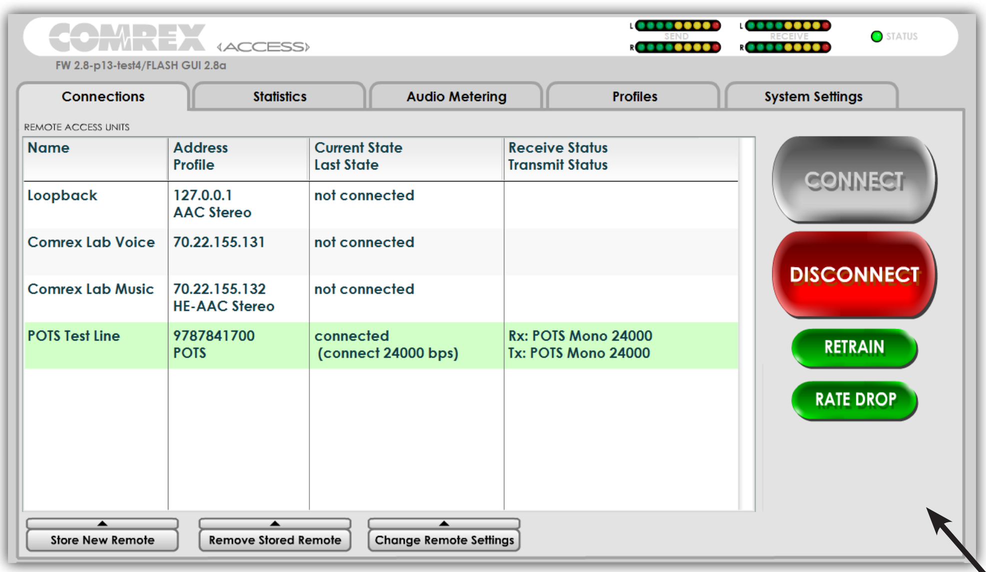
Additional profiles may be built utilizing the normal POTS codec modem mode, if desired. You can then build two remotes to the same phone number — one using your stereo profile and one using your legacy compatible POTS codec profile.

Incoming unit settings (usually the studio unit) – The incoming unit will receive the call from the field. In this case, the ACCESS must be configured to treat all incoming calls as *POTS Stereo Mode*. This is done in the **System Settings** section by selecting **Modem Mode** under **Modem Settings.** To receive stereo calls, this setting must read "Stereo POTS". To receive calls from older Comrex POTS codecs (or ACCESS configured to emulate them) the setting must be "POTS Codec".

Rate Drop vs. Retrain

When incoming or outgoing POTS calls are active, the **Connections Tab** changes slightly. You will see two additional buttons appear on the tab, labeled **Retrain** and **Rate Drop**. These are special functions applicable only to POTS calls, so they are not visible during IP connections.

The **Connection Tab** display contains two user controls, **Rate Drop** and **Retrain** (#1 in Figure 34). These controls are similar in function to those provided on POTS codecs. ACCESS will initially connect at the best data rate supported by the telephone line, and will display that connect rate on the **Connections Tab** page.



1

Figure 34 - Connections Tab During an Active POTS Call

You can force the system to drop to the next lowest connect rate at any time by clicking the **Rate Drop** button at any time. Audio transfer will be interrupted momentarily while the units negotiate the new connect rate. Alternately, you can force the system to initiate the entire training sequence

again (the "chat" sounds heard at the beginning of a call) by clicking the **Retrain** button. You will lose audio for a longer time (approx. 7 seconds) but the modems will completely re-equalize the connection and return audio when finished.

Once ACCESS has dropped to a lower rate, either by rate drop or retrain from either end, there is no way to force it to connect at a higher rate. If you want ACCESS to try again for a higher connect rate, you will need to disconnect the call and dial again.

TROUBLESHOOTING POTS CONNECTION

There are dozens of factors that can affect the success or failure of a POTS codec call, some within the user's control and some not. Here's a short list of rules to follow for POTS codec connections:

1. Use the POTS codec on a direct telephone company line and avoid in-house phone systems. A line used by a fax machine usually provides this direct access. (Be sure to disconnect the fax machine before connecting the codec!)

2. Check to see that there are no extensions or modems on the line you are using — or at least arrange that no one uses these during your broadcast.
4. If there is call-waiting on your line, disable it by entering *"*70"* in front of the number you are dialing.

5. If possible, try the POTS codec out at the remote site before your actual broadcast at about the same time of day that you plan to use it. This will give you a good idea of expected connect rates and possible line problems.

6. At minimum, connect a few minutes before airtime to assess the connection quality. Setting a MaxRate on the POTS codec, based on your findings, is highly recommended. MaxRate usually should be set at a level or two below the maximum unrestricted rate. This will provide a "guard band" of sorts against noise and corruption which may cause errors on the line.

7. If operation starts to degrade after a long period of connection, it may be that the phone line parameters have changed. These parameters are affected by factors such as time of day, weather and geographic location. The modems should be given the opportunity to renegotiate for these new parameters.

8. If you experience low connection rates or errors, try redialing. If that does not help, dial from the other end. If the call is long distance, try forcing the call to another carrier. If a good connection is found, keep that line up.

SECTION 10 SWITCHBOARD TRAVERSAL SERVER (TS)

The Switchboard Traversal Server is a service built and maintained by Comrex on the public Internet that provides users a directory of other users, facilitating connections to devices that would normally have trouble accepting incoming IP connections. Use of the Comrex Switchboard TS is free and comes activated from the factory. The next section describes the theory of Switchboard TS. If your primary interest is in enabling and using it, skip to the section labeled *CONFIGURING Switchboard TS*.

Switchboard TS is useful because it's not always the simplest thing to connect two devices which are essentially "peers" on the Internet, and there are two major reasons why. First of all, to initiate a stream to a device on the Internet requires that you know its IP address. This is the number that gets applied to the destination field of the IP packet, so the Internet routers can figure out how best to send it along its way. Every device that connects directly to the public Internet must have one, but when web browsing or sending email this information is usually hidden from the user. In the traditional client/server scenario, (like web-surfing) a Uniform Resource Locator (URL) is used to represent the IP address of the web page (which is decoded by a DNS server). Once a computer requests a web page from a web server, the web server can automatically derive the reply address from the request and respond to it. So the traditional four segment decimal address (e.g. 70.22.155.130) is completely obscured to the user.

Even if you know your IP address, it's quite possible that address will change over time. This is because the vast majority of Internet users establish their addresses via DHCP, a protocol whereby a server (maintained by the ISP) will deliver one of their available addresses to the client on initial connection. That address is "leased" from the server for a particular time period, and after the lease expires the server is free to change it.

The commonly encountered NAT (Network Address Translation) router adds to the confusion, making codecs even harder to find. Most LAN-based Internet connections (as opposed to computers connected directly to ISPs) actually negotiate with a local router containing its own DHCP server. This router assigns the LAN computer or device a "private" IP address. We'll cover more about the challenges of connecting codecs behind NAT routers shortly, but one of the hassles they add is that the private IP address delivered to the codec (and the only address of which the codec is aware) has no bearing on the public address seen from the Internet. As shown in Figure 35, in extreme scenarios several layers of address locality can be stacked, assuring that the IP address assigned to your is several degrees removed from the public IP address used for connections. And of course, each address in the stack is temporary and able to change at any time.

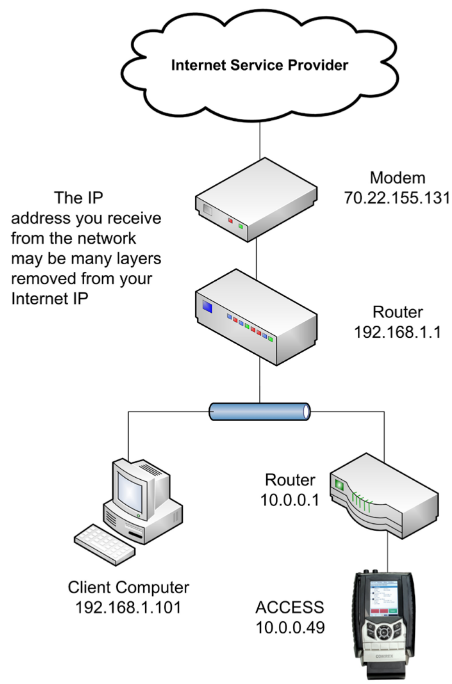


Figure 35 - The Effect of NAT

Before deployment of the Traversal Server, the answer to this dilemma has been to assure that the codec located in the studio has a fixed, public IP address. By fixed, we mean that the address is allocated exclusively by the ISP, and that address is entered manually into the configuration of the codec and not subject to change. This scenario works because IP "calls" are usually initiated from the field. As long as the field unit can find the fixed address of the studio unit and send a stream to it, a reverse channel can be created easily and automatically by the studio unit using the source information contained in the incoming packets. Of course, even in this scenario the studio IP address must be memorized or input into each codec individually.

The first function of the Traversal Server works around the dynamic IP address problem by acting as a Directory Server. Codec users simply log in to the free server and are given an account name and password. Once logged in, it's a simple process to input the details of each codec owned. On the codec itself, the user will input a familiar name by which the codec will be known within that group. See the *CONFIGURING SWITCHBOARD TRAVERSAL SERVER* section for instructions on how to log in to the server.

Once enabled, whenever a codec in the group gets physically connected to the Internet (by any means—3G card, satellite, Ethernet etc), the unit will sync with the server. The current public IP address of the codec will be obtained by the server and the user directory will be updated with the new IP. In addition, the availability status of the codec is also updated. The codec will "ping" the server if anything changes (address, status, etc). As we'll see, this "ping" function will prove useful in other ways.

Once the codec has updated its status with the server, it's time to download the directory. This process happens instantly. The update includes current addresses and status info for all codecs within the group. As shown in Figure 36, this information forms a sort of "Buddy List" that gets integrated into the codec's connection address book. The list may still consist of entries made manually by IP address into the codec, but those are signified by a different icon. Current status of each codec is reflected by graying out entries which are not currently connected or that haven't been synchronized to the server for any reason. As shown in the diagram, IP addresses are not displayed at the first level, as they are no longer important to the user. If the address should change, the codec will re-sync with the server from the new address, and all will be updated. Connections can be made by simply clicking on the correct name, regardless of current IP address.

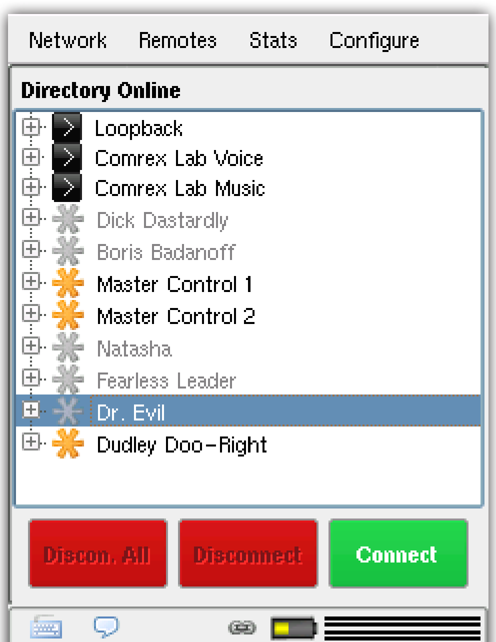


Figure 36 - Switchboard TS Buddy List

The other roadblock provided by the use of NAT routers is the inability to accept unsolicited incoming connections from the Internet. In a general sense, this function acts as a rudimentary firewall and is a net positive for security, but it does cause headaches for codec users. As shown in Figure 37, a router that receives a connection request doesn't have a clue where to forward that stream unless it has specific instructions programmed into it, known as "port forwarding." This can work well for fixed installations, but it's not always an easy task to obtain that kind of security access on corporate routers, and forwarding functions are implemented differently on different hardware. You can easily imagine the complications of obtaining or managing port forwarding on the LAN at each remote venue, you would certainly encounter a high volume of grumpy IT staff if you tried.

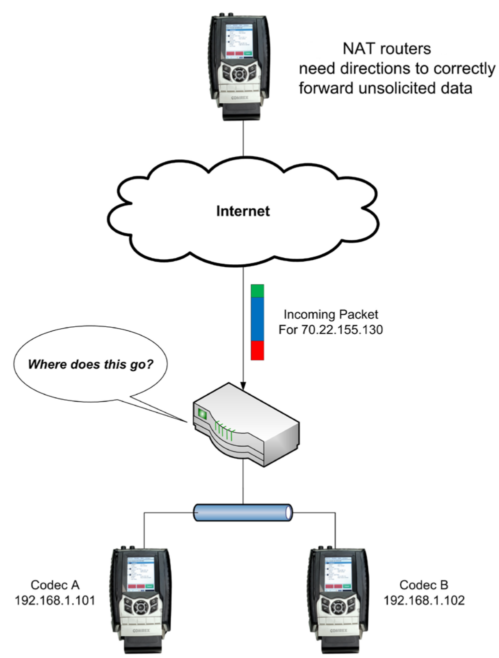


Figure 37 - Incoming Packets Hitting NAT Router

In describing NAT routing, it's important to understand the concept of ports. These are numbers, like the source and destination IP addresses that are attached to each packet to further qualify which application on a computer (or codec) is meant to send or receive a packet. In a typical codec application unit X will send a packet from address A port B to address C port D on the destination codec Y. A codec that has multiple applications running (like streaming audio while simultaneously serving a configuration web page) would deliver these applications from and to different port numbers, but perhaps to the same IP address. Port numbers are also used by NAT routers in segmenting applications flowing through them and they may change source port numbers at will.

Network Address Translation (NAT) refers to the ability of a router to translate requests from computers (or codecs) within its LAN onto the public Internet. On its most basic level, this involves replacing the private "source" or return IP address in each packet with the true public IP and remembering where that packet was sent so that any response can be forwarded back to the proper device. A good metaphor for this would be that an outgoing packet punches a hole in the router, through which authorized reply packets may be returned to the codec for a limited time, as shown in Figure 38.

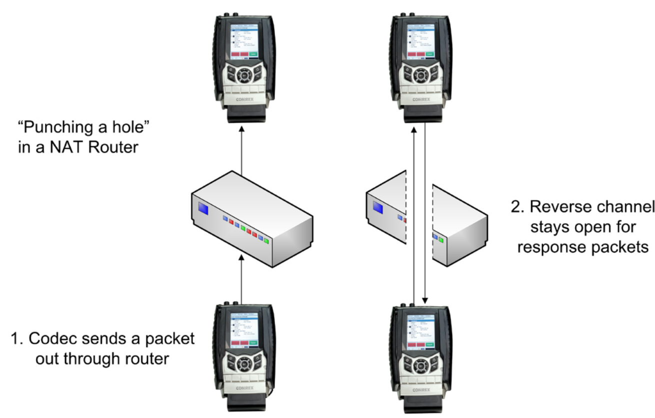


Figure 38 - "Punching a Hole" in a NAT Router

The Traversal Server aids in breaking through these different types of routers for incoming calls. Because it is in constant contact with all subscribed codecs, it can send and receive test patterns to determine whether one or more NAT routers exist on a link and what type they are. It can then choose a connection method to be used to circumvent the problem. Options available to it include:

- Instructing the calling codec to make a normal connection (No NAT detected).
- Using the hole punched by connection to the Directory Server for incoming connections from other codecs.
- Instructing the called codec to make the connection in the reverse direction.

The second option, which utilizes the outgoing Directory Server "ping" described earlier, is very useful. The interval of this ping is adjustable, but defaults to about one minute, which is short enough to keep a hole punched through the majority of NAT routers.

These techniques are based loosely, with enhancements, on a generic Internet protocol called STUN (Simple Traversal of UDP through NAT). The system works well in all environments except one—when both users are sitting behind a symmetric NAT. In this situation calls will fail even with Traversal Server. The only option in that environment is to resort to port forwarding on one side of the link.

Configuring Switchboard Traversal Server

Switchboard TS is licensed to your codec when delivered from the factory. An account on the Switchboard TS is required and can be obtained by contacting Comrex at 978-784-1776 or 800-237-1776 or by emailing techies@comrex.com or info@comrex.com.

Settings can only be changed via the *Console Connection Interface*. The Traversal Server setup page is found in the **Traversal Server** section of the **System Settings** menu, as shown in Figure 39.

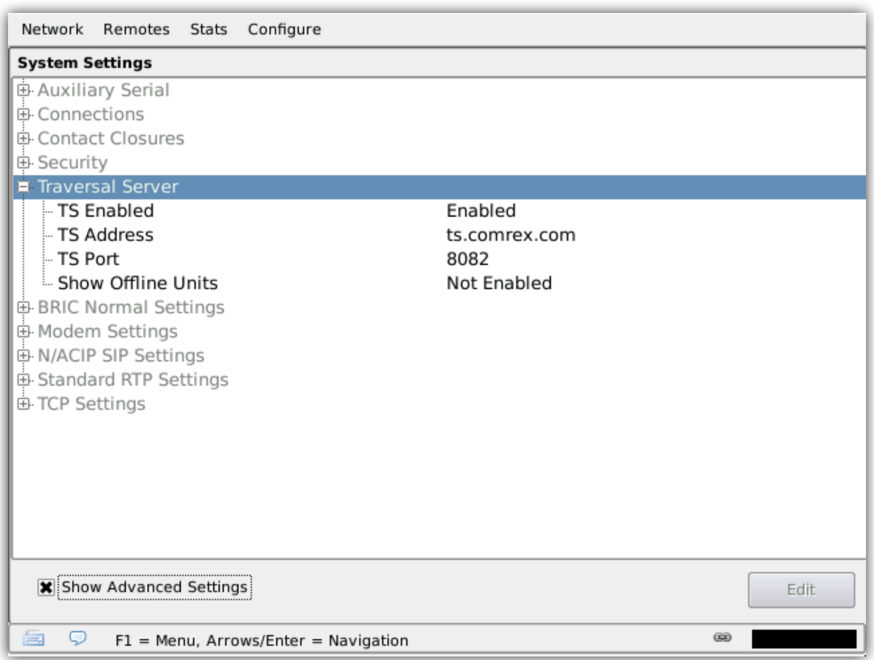


Figure 39 - Traversal Server Settings

The **TS Enabled** setting enables the Switchboard TS function on this codec. If this option is disabled, the codec will no longer use the server.

The **TS Address** setting allows you to enter the address of the Traversal Server, which defaults to ts.comrex.com. This is unlikely to change but if you intend to set up a private server, you'll need to enter the address of your server here.

The **TS Port** setting allows you to enter the TCP port of the Traversal Server, which defaults to 8082. If you are using a private server, you may need to change the port for your server here.

Show Offline Units is the final setting which determines how other codecs in your group are displayed. If this is enabled, all codecs in the group will always appear on the **Remotes** list, including units that can't be located being greyed out. If disabled, non-locatable units will not appear.

If you wish to change the name of your ACCESS unit as it appears to other Traversal Server peers, you can set it via the **Unit Name** option of **Connections** in the **System Settings** menu.

Logging in and Setting up the Switchboard Traversal Server

In order to use Switchboard TS, you must first have an account with the server. A user name and password will be provided by Comrex. You can log in to switchboard.comrex.com using that information. Once you've logged in, we advise clicking **Account Info** and adding the information about the owner of the account. You may also change the account password in this section.

The first time you log in to Switchboard TS, you will see a notice stating that no units have been added to the account yet. By clicking on **Add New Unit**, you will be prompted to input the Ethernet MAC address of the ACCESS you wish to add. The MAC address is available via the touch-screen under **Network->Configure Network**, or alternatively by scanning for the unit via the Device Manager PC based software utility. The MAC address of the ACCESS must be inputted in a format with colons between each pair of characters.

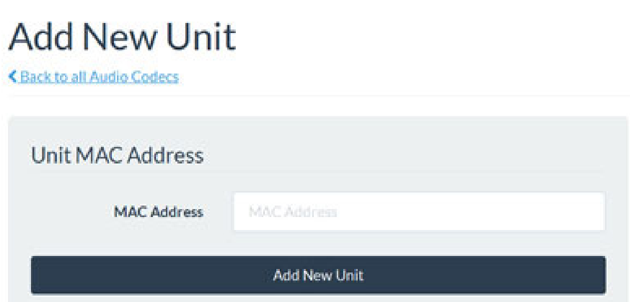


Figure 40- Entering New Units

Once the unit's MAC address(es) are input correctly, you will see them appear in the unit list as shown in Figure 41. The next time the properly configured codec goes on-line, it will sync with the server. The codec name, AAC status and other information will be updated.

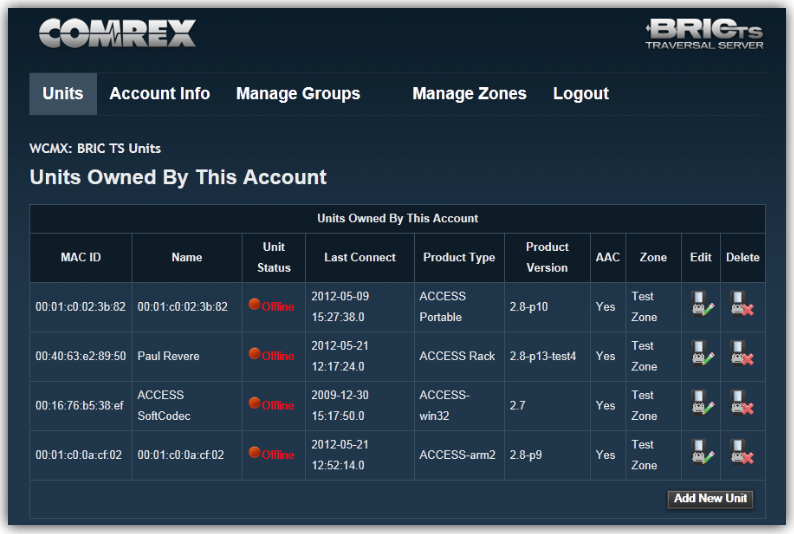


Figure 41 - Switchboard TS Main Account Screen

Using Switchboard TS

Once Switchboard TS is enabled and you have correctly created your group on the server, you will get a download of the all other codecs in your group to your **Remote List** as shown in Figure 42. On the *Web-based Interface*, Switchboard TS entries are shaded as shown in Figure 43.

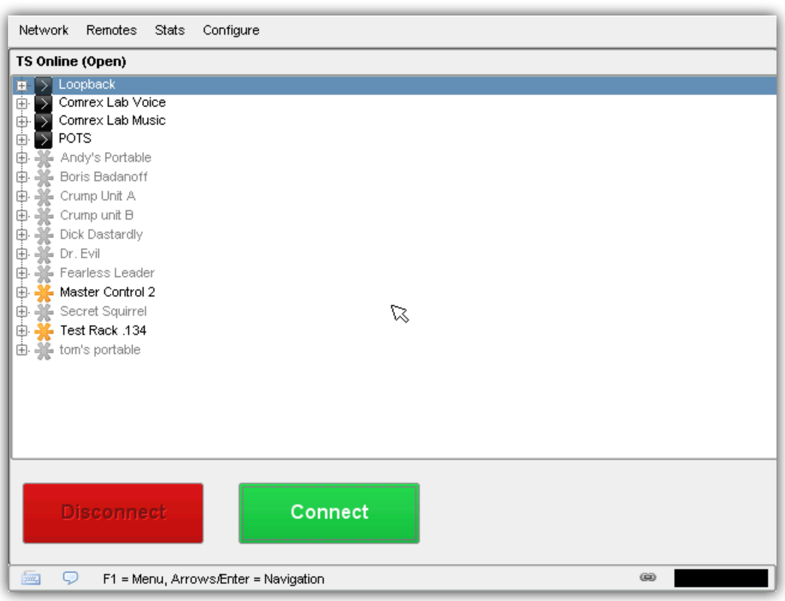


Figure 42 - Switchboard TS Remote List

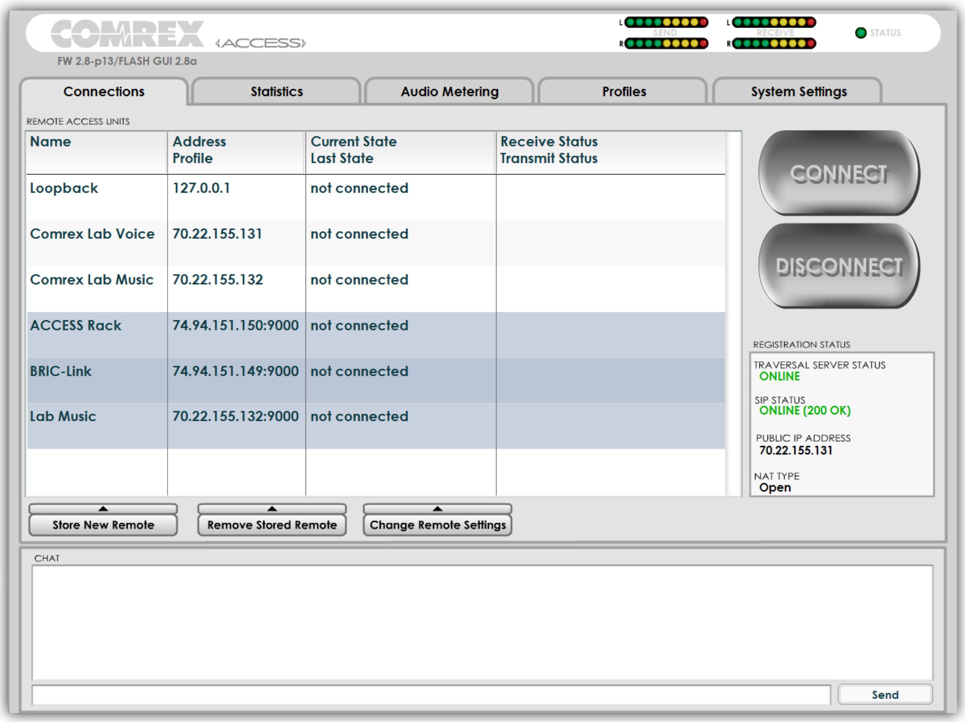


Figure 43 - Switchboard TS Entries on the Web-based Interface

In addition, on the *Console Connection Interface* the type of NAT router that is detected will be displayed on the top bar of the **Remotes List**. The choices are:

1) Open - No NAT detected, unit sees the Internet directly.
2) Symmetric NAT or FW - The most challenging type of router or firewall for codec connection purposes. If both ends are behind this type of system (and no port forwarding is applied) connections will not work.
3) Full Cone, Restricted or Port Restricted NAT - Switchboard TS can usually work around this type of router, allowing calls to be placed in both directions.
4) UDP blocked - No normal codec connections are possible through this router.

To make calls with the help of Switchboard TS, simply click one of the entries with the orange TS icon (or shaded entry in the *Web-based Interface*) and click **Connect**. Switchboard TS will handshake with the remote unit and make the connection automatically.

CREATING USERS

In some situations, you may wish to create additional Switchboard users who can access the server web interface. You can do this via the “Users” tab at the top of the main codec list. This allows you to create accounts for users that can later be deleted if no longer desired. As shown, several user accounts can be created with unique passwords.

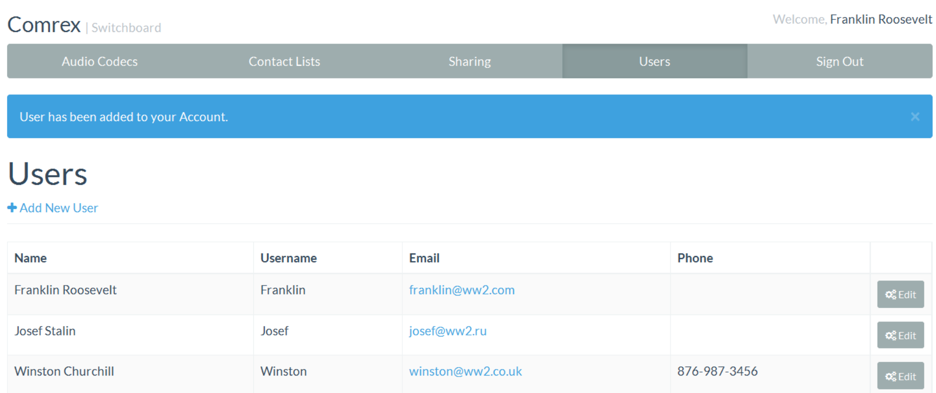


Figure 44 - Switchboard Users List

CONTACT LISTS

In some situations, it might not be desirable for every codec in your fleet to see the Switchboard status of every other codec. To help filter what’s displayed on a codec’s interface, Switchboard has implemented the concept of “Contact Lists”. Contact Lists contain a subset of your codec fleet on your account. You can create multiple Contact Lists that consist of different subsets. With the exception of Shares (discussed next), only units within your Switchboard account may be assigned to Contact Lists.

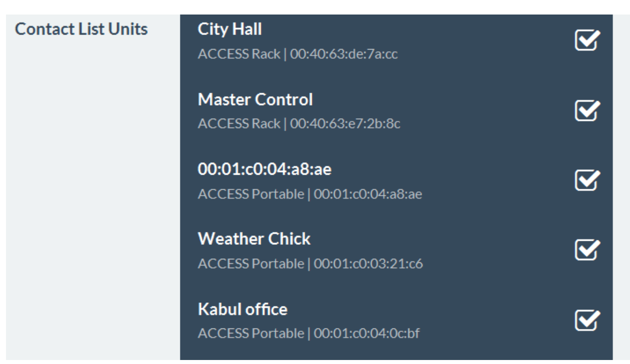


Figure 45 - Switchboard Contact Lists

By default, a master Contact List is created that contains all codecs on your account. And by default, every codec in your fleet uses the master list. So if you're not interested in segregating codecs on your account, the default configuration will work fine.

You can create multiple Contact Lists, each with a subset of your codecs, and save them on the Switchboard server. You then have the ability to assign these lists to your codecs. This will reduce the number of devices displayed on that unit to the codecs on the Contact List.

This is an important point. Assigning a Contact List to a codec determines what gets displayed in its own list. It does not have any impact on how that codec is displayed on other devices.

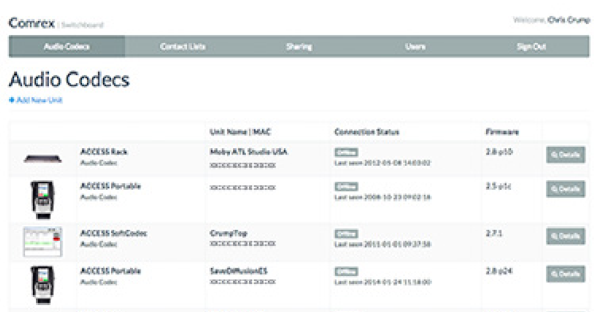


Figure 46 - Changing Active Contact List

As shown, in the Switchboard web interface you can select one of your individual codecs and change the "Active Contact List" from default. This will change the list of codecs displayed on that unit.

Shares

In the case where you'd like to allow users outside your account see the status of some devices in your fleet, Switchboard has implemented Shares. Shares are subsets of your codec fleet that you define. Once defined, you can invite other Switchboard accounts to add your Shares, and your codecs become visible to them.

Shares are a one-way transaction. If you invite an external user to share, and he accepts, you don't get any additional status on your codecs. The external users must create a share and invite you for the share to be two-way.

Shares are created by clicking the top tab entry labeled **Shares.** A list of your current Shares appears and you can added more by clicking **Add New Share**.

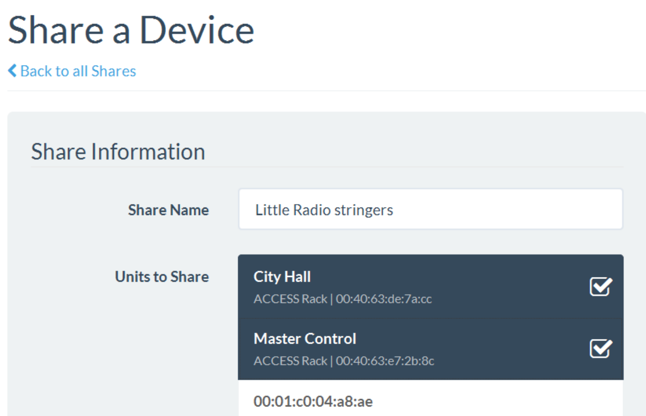


Figure 47 - Share a Device

The share creation screen allows you to choose a subset of your fleet for this share.

After you make your selection, you'll need to enter either the name of the account you wish to share with, or the email address of the administrator of the account (it must be the one they used to create their Switchboard account). An email will be sent from the server asking the user to confirm your Shares.

Once the Shares are confirmed, your shared devices will appear as options in the external user's contact list menu. This is important: Shares do nothing until the external user adds them to a contact list. If the user has only a single (default) contact list for his fleet, he must still manually add your codecs to that in order for them to be visible to his fleet.

Finally, if you want to temporarily deactivate a share, this can be done by editing the share entry. A tick-box on the bottom allows activation/deactivation of a share without the need to delete it or re-invite users.

Section 11 About the Algorithms

ACCESS contains several different types of encoders and decoders for use on networks.

BRIC-HQ1
(High Quality 1)

This encoder/decoder provides 15 kHz voice/music transmission with extremely low delay and low network utilization. It supports mono, stereo, and dual-mono. Here are some details of *BRIC-HQ1*:

- **Low Delay —** *BRIC-HQ1* uses a 20mS audio frame, with an overall encode/decode time of around 60mS. This makes BRIC-HQ1 a good choice for real-time, interactive applications.
- **Low Digital Bandwidth —** *BRIC-HQ1* has a data rate of around 24 or 28 kbps for mono, and 56 kbps for dual mono allowing it to travel over medium-to-low speed networks.
- **Voice/Music Capable —** *BRIC-HQ1* is designed as a voice codec, but does a respectable job at encoding music.
- **Dual Mono Mode —** Supports the encoding of two independent audio channels, such as a dual-language broadcast. These two channels will be multiplexed into a single outgoing stream.
- **Stereo Mode —** This mode uses matrixing to deliver stereo audio at less than double the bandwidth.

BRIC-HQ2
(High Quality 2)

This encoder/decoder provides high fidelity (12 or 15 kHz) mono or stereo transmission at low data rates and reasonable delay. Here are some details of *BRIC-HQ2*:

- **Medium Delay —** *BRIC-HQ2* uses a 64 or 80mS audio frame, with an overall encode/decode time around 260mS. Interactive applications are possible using *BRIC-HQ2* in the forward direction and *BRIC-ULB* or *BRIC-HQ1* in the reverse.
- **Low Digital Bandwidth —** *BRIC-HQ2* encodes at 24 kbps for a full bandwidth mono signal. Stereo signals occupy 30 kbps. Dual mono is not supported in *BRIC-HQ2*.
- **Voice/Music Agnostic —** *BRIC-HQ2* utilizes a blend of different audio coding techniques, so it does a good job of encoding non-voice audio.
- **Mono/Stereo —** *BRIC-HQ2* has stereo modes which utilize a parametric stereo effect; so it is not possible to send independent audio over the L&R channels. The channels must be a related stereo image. Use *BRIC-HQ1* or *AAC-LD* when *Dual Mono* is required.
- **Audio Bandwidth —** *BRIC-HQ2* default modes utilize a 32 kHz sampling rate to deliver 15 kHz audio fidelity. BRIC-HQ2 12K modes utilize a 26 kHz sampling rate to achieve a 12 kHz audio fidelity. Because the data rate is the same between the two modes, *BRIC-HQ2 12K* can be considered to sacrifice some slight high end fidelity in exchange for overall lower audio coding artifacts.

BRIC-ULB
(ULTRA LOW BITRATE)

This encoder/decoder provides 7 kHz voice audio transmission with extremely low delay and extremely low network utilization. Due to its low digital bandwidth, it is considered to be the most robust mode for use on constrained networks. Here are some of the details of *BRIC-ULB*:

• **Low Delay** — *BRIC-ULB* uses a 20mS audio frame, with an overall encode/decode time of around 75mS. This makes BRIC-ULB a good choice for real-time, interactive applications.
• **Low Digital Bandwidth** — *BRIC-ULB* has a data rate of around 12 kbps, allowing it to travel over very low speed networks. Also, since BRIC-ULB is so efficient, error correction may be added in many situations without congesting the network.
• **Vocoder** — *BRIC-ULB* relies on a voice based vocoder, which is the same principal utilized in many digital mobile phones. The difference is that while mobile phone vocoders typically provide about 3 kHz audio bandwidth, *BRIC-ULB* delivers more than twice that fidelity, providing a much more listenable and less fatiguing sound. *BRIC-ULB* is optimized for human voices. It does a respectable job of encoding background noise and crowds, but music tends to suffer rather dramatically on *BRIC-ULB*.
• **Mono** — Only a single audio channel is supported on *BRIC-ULB*.
• **Dynamic Data Rate** — The *BRIC-ULB* encoder adapts its outgoing audio frame size based on the complexity of the incoming audio.

LINEAR PCM

This encoder does not compress audio at all. It uses a 48 kHz sampling rate and simply applies small frames of linear audio to IP packets. This mode is only useful on high bandwidth LAN or managed WAN environments. *Mono Mode* requires a network capacity of 768 kbps while *Stereo Mode* requires a network bandwidth over 1.5 Mb/s.

FLAC

This encoder compresses the audio data using a lossless algorithm. This means that the audio extracted from the decoder is identical to the audio input to the encoder, with no coding artifacts. FLAC typically removes 30-40% of the network data compared to Linear PCM, but the actual data rate is variable and is based on the complexity of the coded audio. Using FLAC over Linear PCM typically results in a slightly higher (5ms) overall delay.

G.711

G.711 (μ-law and a-law) — These are the coding algorithms used by standard digital POTS calls, and provide about 3KHz (telephone quality) audio. μ-law is utilized in North America, while a-law is prevalent in Europe. These algorithms are provided for compatibility with SIP-style VOIP phones, but don't provide much benefit over standard telephony in audio terms.

G.722

G.722- This is a well known 7KHz (medium fidelity) algorithm used in some VOIP telephones and codecs. It is provided for compatibility purposes, but is not considered a superior algorithm for audio codecs.

AAC

This algorithm is a highly regarded standard for compressing audio to critical listening standards. It has been judged to produce "near transparent" audio at a coding rate of 128 kbps stereo. The standard is a collaborative of several audio companies best efforts, and has become popular as the default audio codec of the Apple™ iTunes™ program. AAC should be considered the highest quality codec in ACCESS—Enhancements like HE-AAC and AAC-ELD attempt to maintain a similar quality and reduced bandwidth and delay.

HE-AAC

This is a newer version of AAC defined for increased efficiency. The goal of the algorithm is to produce AAC comparable quality at a lower bit rate. It does this by encoding lower frequencies to AAC, and higher frequencies using Spectral Band Replication (SBR), a technique that partially synthesizes these high frequencies. HE-AAC is trademarked by other companies as AACPlus™. HE-AAC (and close derivatives) are often used as the main audio codec for digital radio and satellite networks.

HE-AACv2

This algorithm further increases the efficiency of HE-AAC by adding intensity stereo coding. This results in a lower bit rate for stereo signals. We also cluster a very reduced rate HE-AAC mono into this category, although technically it does not contain v2 coding.

AAC-LD

This algorithm is an extension of AAC developed by the FhG IIS, who are the contributors to AAC and primary inventors of the MP3 algorithm. It's quality is superior to MP3 at similar bitrates (64-128 kbps) but it exhibits very low delay (100mS). This choice is best when reasonable network throughput is assured, near-transparent audio is required and interactivity is needed.

AAC-ELD

This latest algorithm is a combination of the LD and HE AAC variants. It provides the network conserving benefits of SBR along with the dramatically reduced delay time of LD. For low delay applications, it's usually the best choice.

SECTION 12 MULTI-STREAMING

ACCESS supports the ability to run one encoder per box. But this single encoder stream may be sent to up to nine destinations simultaneously. We call this capability multi-streaming, since the encoder creates a separate but identical outgoing stream to each decoder. *Note: Your Internet connection must be able to support these streams. For example, if your encoder runs at 35 kbps network utilization, sending to two locations will require 70 kbps upload speed from your network.*

Multi-streaming should not be confused with IP Multicast, which is described in the next section.

Each ACCESS can also run only one decoder. So it's important that in a multi-stream environment, a maximum of one stream is sent in the reverse direction. This means that users interested in hearing a multi-stream must turn off their encoders.

This can be a bit confusing because multi-streams can be initiated from either end of the link.

Figure 44 shows an ACCESS multi-stream arrangement. ACCESS A is the multi-streamer, with ACCESS B, C and D listening to the same audio. In order to set up a multi-stream scenario, you will need to know how to turn ACCESS encoders **Off**. This must be done by building a profile with either the **Local** or **Remote Transmitter** mode set to **Off**, as shown in Figure 48.

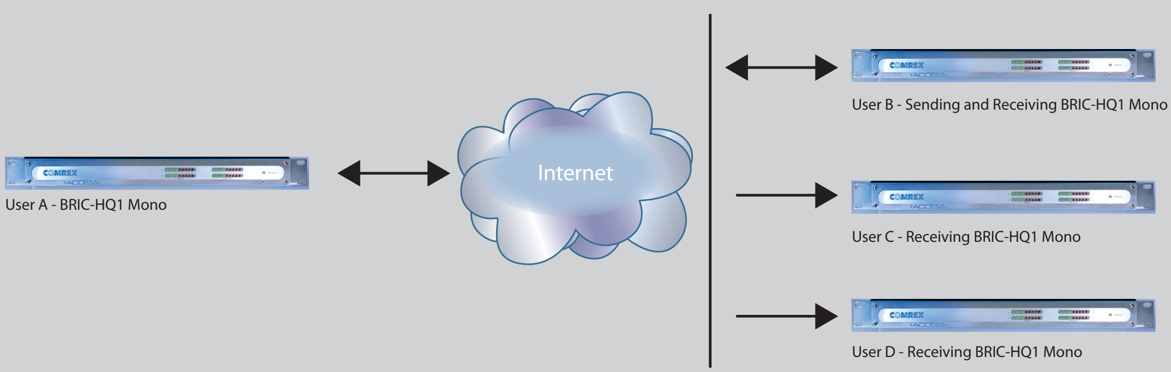


Figure 48 - Multi-Streaming Arrangement

We'll give two examples of multi-steaming scenarios. The first is an environment where the ACCESS that is serving the multi-stream initiates the calls, and in the second the serving ACCESS accepts all its incoming connections.

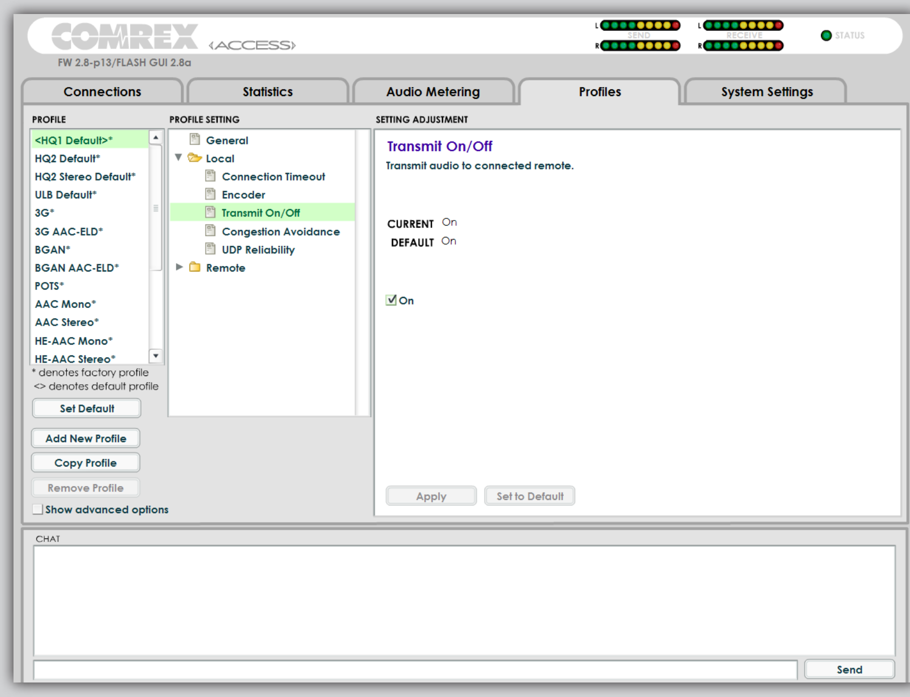


Figure 49 - Transmit On/Off in the Profiles Tab

In the "multi-streamer as caller" model, two different profiles will be built on ACCESS A. The first profile, labeled "Multi-Duplex," will be defined as a normal, full-duplex ACCESS connection. The encoder to be used will be selected in the **Local Encoder** section, and the stream desired in return will be defined in the **Remote Encoder** section.

The second profile is called "Multi-Simplex" and in this profile the **Remote Transmitter** is turned **Off**. Most other selections in this profile are irrelevant.

User A will define remote connections for ACCESS B, C, and D. He will assign the "Multi-Duplex" profile to ACCESS B, and "Multi-Simplex" profile to the others. He will then establish a connection with ACCESS B first, followed by C and D.

In model number 2 where the serving ACCESS accepts all incoming connections, all the profiles are built on the **Remote Receivers**. ACCESS B will use a simple profile by defining the encoders in each direction, and assign it to ACCESS A. ACCESS C and D will each define a profile with their **Local Encoders** turned **Off**, and assign them to A. ACCESS B should connect first. When C and D connect, they will hear the same stream as B, regardless of how their remote encoders are set in their profiles.

In a multi-streaming environment the first man wins. For example, the first connection made between units will determine the encoders used for all others. After the first full-duplex connection is made, all other attempts at full-duplex connections to either end will be rejected.

SECTION 13 IP MULTICAST

Warning: Advanced Topic

IP Multicast is an efficient way of delivering ACCESS digital audio streams to multiple locations. This involves relying on the network to distribute the stream to the locations that require it, rather than creating an independent stream for each user.

IP Multicast requires the use of an IP Multicast-capable network. The commercial Internet, with few exceptions, is not capable of supporting IP Multicast. Some private LANs and WANs are IP Multicast capable.

IP Multicast supports only a single direction stream. An IP Multicast encoder can not receive input streams.

In this manual, we assume that IP Multicast users will be familiar with the basic concepts of setup and operation of the network, so we will focus on how to configure ACCESS for Multicast mode.

MULTICAST PROFILES

To set any remotes to Multicast, you must first create a profile for either a Multicast Sender or a Multicast Receiver on the **Profiles Tab**.

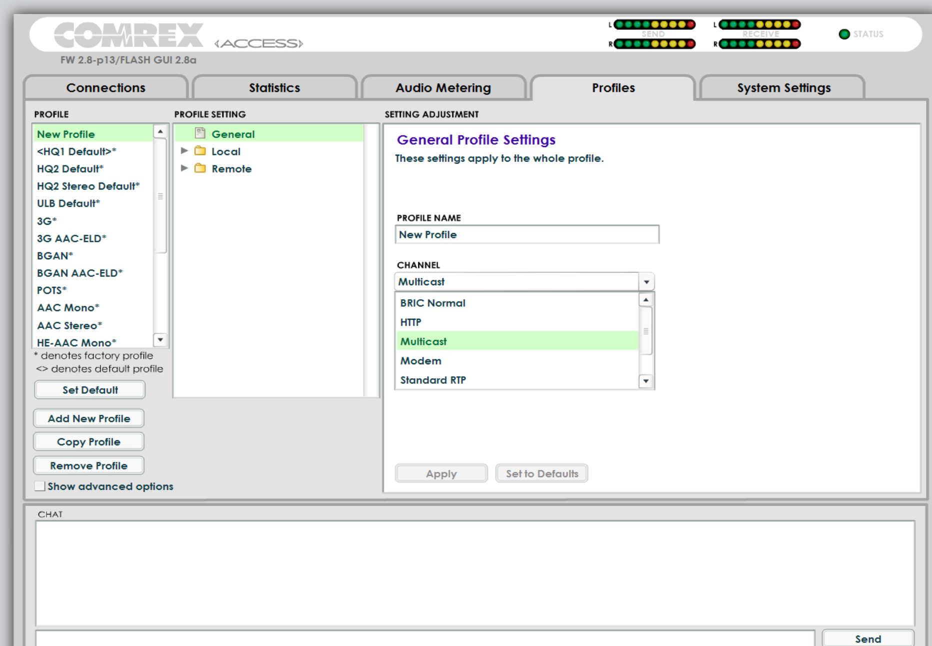


Figure 50 - Multicast Selection in the Profiles Tab

As shown in Figure 50, when you define a new profile, you have the option to choose **Multicast** as the profile type. Multicast profiles have fewer options than other profile types, and some of the available options will have no effect (e.g. setting an encoder type on a Multicast receiver has no effect). The important settings for Multicast are:

• **Sender/Receiver** – Determines whether this particular ACCESS is designed to generate the IP Multicast stream (send) or decode one (receive).

• **Encoder Type** – Determines the type of stream to be used by the Multicast Encoder—not relevant for decoders.

In addition to the basic options for IP Multicast profiles, clicking the **Advanced** box will allow setting of the same **Advanced Options** available for Normal BRIC (Unicast) profiles. See the *Profiles Tab* section for more information.

Setting up a Multicast Remote

All Multicast connections are outgoing connections — A Multicast Sender must initiate an outgoing stream, and a Multicast Receiver must initiate an incoming one. These remotes are configured within a special address range known as a Multicast Block, typically 224.0.0.0 to 239.255.255.255. To establish a Multicast connection, simply define a remote as having an address within the IP Multicast Block, use an IP Multicast profile, and press **Connect**.

Time-to-Live

Time-to-Live (TTL) is a variable set by Multicast encoders to determine how long a packet is processed before it is dropped by the network. The default value of TTL in ACCESS is 0, which limits its use to within a LAN environment. TTL may be manually changed on a Multicast Sender remote by configuring the IP address followed by a “/”, followed by the TTL value. An example remote Multicast encoder could be set for the address 224.0.2.4/255, which would signify an address with the Multicast Block with a TTL of 255 (which is the max value available).

Changing Port Numbers for Multicast

The default port of UDP 9000 may also be changed on Multicast remotes. The port number is assigned in the usual way, directly after the IP address, preceded by “:”, followed by the TTL. As an example, the IP address of a Multicast Sender on port 443 with a TTL of 100 would read:

224.0.2.4:443/100

SECTION 14 STREAMING SERVER FUNCTION

ACCESS has the ability to act as a streaming server, delivering AAC and HE-AAC to compatible PC based media players. Currently tested media players include WinAmp, VLC and Windows Media Player with Orban/CT HE-AAC plug-in.

By default, streaming server functionality is turned off. To enable it, go to the **System Settings Tab** of the *User Interface* and choose HTTP settings option. Under the first option, set **Accept Incoming Connections** to **Enabled**.

Next you will need to choose an encoder for use by the streaming server. Only the encoder choices that are compatible with the players listed are shown in this menu. Choices span between a mono audio feed at 18 kb/s, up to a stereo feed at 128 kb/s. Keep in mind multiple streams will require this bandwidth along with around 25% overhead for each stream.

The **Genre**, **Info URL** and **Public** options may be set for anything, or left alone. These options, if applied, will be embedded into the stream.

DECODING A HTTP STREAM

To decode a stream, open one of the supported players and find the option to open a URL based stream. In Winamp and VLC, input the address of the ACCESS in the following format:

http://192.168.0.75:8000
(insert the real IP address, but always use port 8000)

In Windows media, input the address like this:

http://192.168.1.75:8000/stream.asx
(using the actual IP address, of course)

SIMULTANEOUSLY CONNECTING ACCESS AND STREAMING

ACCESS can stream while connected to another ACCESS in normal mode. If the BRIC connection is using an *AAC* algorithm supported by players, when a stream is requested it will be delivered using the same encoder as the BRIC connection, regardless of the HTTP settings. If the ACCESS encoder is *Linear* or *FLAC*, the stream request will be rejected.

SECTION 15 GATEWAY OPERATION

About Gateway Operation

ACCESS includes a special operational mode that allows it to share a network connection with other devices. ACCESS will create and maintain the main network channel, then act as router over a second network port to deliver data to an external device.

ACCESS codec packets contain real-time headers, and the ACCESS will deliver these to the network ahead of other user information. In this way, ACCESS will assure that outgoing user data will not affect outgoing codec packets.

On the return channel, priority of audio codec packets vs. user packets are determined by the Internet Service provider, so if there is contention heavy user data may have an affect on decoder performance.

Connecting as a Gateway

Under most circumstances, ACCESS will be sharing a network with an USB-based network based attached to its **USB** port, and distributing data to other users via Ethernet. In this configuration, you will need an Ethernet switch between ACCESS and the computers getting the data. Alternately, if only one computer will be connected, an Ethernet crossover cable may be used between ACCESS and the computer.

This type of connection is shown in Figure 51. ACCESS is using an USB-based device to connect to the Internet and using its Ethernet port to share the IP connection with a laptop computer via a crossover cable.

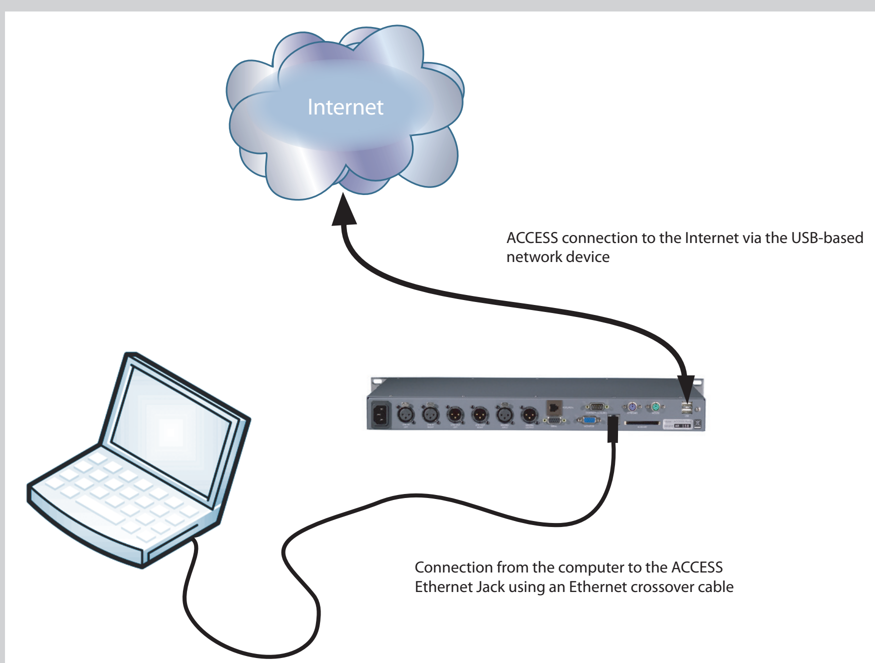


Figure 51 - Gateway Connection

GATEWAY MODE

Gateway Mode involves having two networks active and enabled on ACCESS; The Internet side (usually an USB-based network device) which is used to connect to the world at large, and the shared side (usually Ethernet), which is used to connect with other computers.

Configuring for *Gateway* operation may only be done through the *Console Connection Interface*. The only step to *Gateway Mode* is setting up your shared network side with the factory default static IP address, network mask and DHCP pool information. Since this is usually Ethernet, this is done in the normal Ethernet **TCP/IP Tab**. Simply select **Gateway** in the pull-down menu (as shown in Figure 52).

In *Gateway Mode*, ACCESS is acting as a DHCP server and router to the other devices. It will assign a dynamic address to all devices connected to it on the LAN. The static address assigned to the ACCESS Ethernet port is 192.168.42.1. The pool of addresses assigned by the DHCP server is 192.168.42.128 - 192.168.42.192.

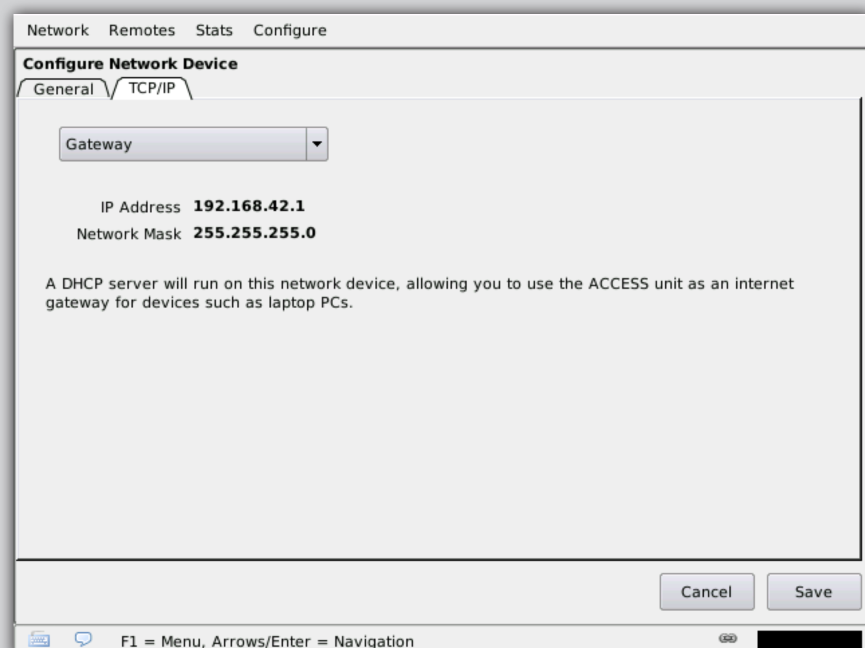


Figure 52 - TCP/IP Tab for Gateway Setup

SECTION 16 MAKING N/ACIP SIP COMPATIBLE CONNECTIONS

Comrex codecs (and many other brands) have a set of protocols that allow easy IP connections between units. In general, when connecting between Comrex hardware, it's best to use these proprietary modes to take the most advantage of the features of the product.

However, many users are concerned about getting "locked in" to a certain codec brand. Because of this, an international committee was formed by the European Broadcast Union called N/ACIP to hammer out a common protocol to interconnect codec brands. This committee resulted in the establishment of EBU3326, a technical document describing how best to achieve this goal.

EBU3326 by and large establishes a set of features each codec should support, then leaves most of the heavy lifting to other, previously established standards like SIP (IETF RFC 3261). Topics not covered (yet) by EBU3326 include things like carrying ancillary data and contact closures from end-to-end, codec remote control and monitoring, and complex NAT traversal, which at this point are still left to the individual manufacturer's discretion. So if these topics are important to your application, it's best to stick to a single codec vendor and their proprietary protocols.

More about EBU3326

The Tech 3326 document defines several mandatory encoding algorithms, and the transport layer that could be used on them for compatibility. But the most complex part of the standard was the decision on how to arrange Session Initialization, which is the handshake that takes place at the start of an IP codec call. The most commonly used protocol is called SIP, which is used extensively by VoIP phones and therefore was a logical choice. SIP carries the advantage of making ACCESS compatible with a range of other non-broadcast products, like VoIP hardware, software, and even mobile phone apps.

EBU3326 in ACCESS

ACCESS does not fully comply with EBU3326, as it does not feature the mandatory MPEG Layer II codec. Aside from this, ACCESS has been tested to be compatible with several other manufacturer's devices using encoders supported by both products. When using *N/ACIP SIP Compatible* mode (this is how the user interface describes EBU3326), ancillary data, contact closures, Switchboard TS, Multi-streaming and Multicasting are not supported. Outgoing call profiles built with the NACIP/SIP channel may lack some advanced options, and can not be set for different encoders in each direction (i.e. N/ACIP SIP calls are always symmetrical).

N/ACIP SIP MODES

A function of placing a SIP-style call is the ability to register with a SIP server. This is a server that exists somewhere on the network, usually maintained by a service provider. Several free servers exist that can offer registration like Gizmo5 and Iptel.

ACCESS allows N/ACIP SIP calls to be placed or received with or without registration on a SIP server. If registration is not enabled, connections are made directly to the compatible device by dialing its IP address, just like in *BRIC Normal* mode.

UNREGISTERED MODE

Placing a call in *Unregistered N/ACIP SIP* mode is simple--just build a profile, but instead of choosing **BRIC Normal** channel, choose **NACIP/SIP**. This will make sure the call is initiated on the proper ports and with the proper signaling. The majority of system settings relating to N/ACIP SIP relate to *Registered* mode.

REGISTERED MODE

Registering with a SIP server in *N/ACIP SIP* mode can have some advantages. When using a SIP server:

- The server can be used to help make connections between codecs through routers
- The remote codec can be dialed by its SIP URI instead of IP address
- The SIP server can be used to find codecs on dynamic IP addresses

SIP SERVERS

A SIP server exists in a domain. This domain is represented by a web-style URL like sipphone.com or iptel.org. A SIP server or proxy generally handles IP connections within its domain.

SIP URIS

The SIP server assigns a fixed alphanumeric name to each subscribed account. For example, an Iptel user may be assigned the user name comrex_user. URIs consist of a SIP user name, followed by a domain, delineated with the @ symbol, like an email address. Our Iptel user's URI would be comrex_user@iptel.org. Comrex devices do not use the designation "sip:" before a SIP address.

If a connection is to be made exclusively within a domain, the domain name can be left off. As an example, to make a call to this codec from another Iptel registered codec, the dialing string can simply be comrex_user (with the domain being assumed).

Registering with a Server

At a minimum, you will need the following information when registering ACCESS with a SIP server:

1) The Internet address of your SIP proxy/server
(e.g. proxy01.sipphone.com)
2) The user name on the SIP account (this is usually the dialing address)
3) The password on the SIP account

Fig 53 shows where this information can be applied in the systems setting section. You will also need to enable the **Use SIP Proxy** option in that menu.

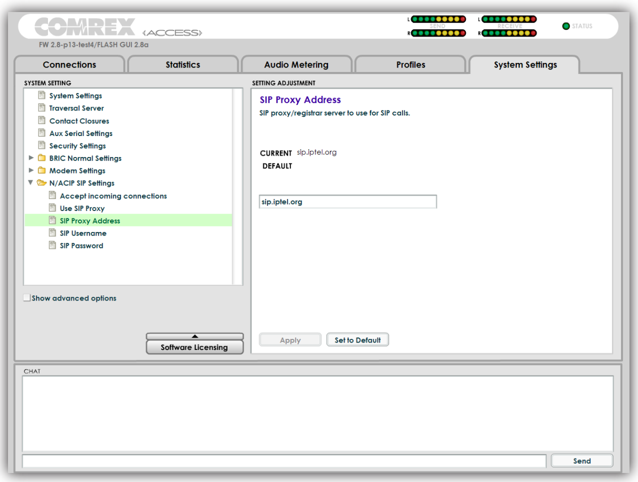


Figure 53 - N/ACIP SIP Settings

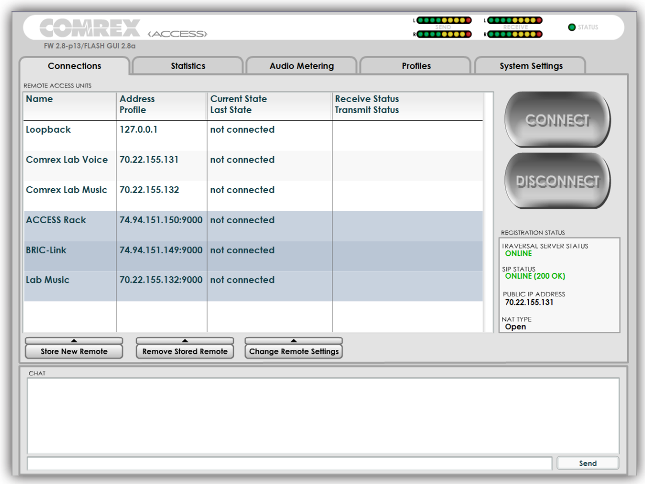


Figure 54 - SIP Status

Once this information is correctly entered, a new field appears in the "Registration Status" box located on the Connections Tab (see fig 54).

The status will reflect the progress of the registration process. When complete, this will display **Online**. If the box does not display **Online** after a short time, it means that registration likely failed. It's best to go back and carefully check the registration info. It might also be useful to be sure the registration information is valid by configuring a VoIP phone or softphone with it and see if that registers.

SIP registration can be very simple with some servers, and others can require more advanced settings. There are several advanced settings available for use with SIP and they are described in the *ADVANCED TOPIC* sections.

MAKING SIP REGISTERED CALLS

When registered, calls made using a N/ACIP SIP profile behave differently than normal. The address field, regardless of whether it is a SIP URI or an IP address, is forwarded to the server. No connection attempt is made until the server responds.

If the server accepts the address, the call will be attempted. If not, an error message will appear in the status line. Reasons for call rejection by a server are many. Some examples:

1) The server does not support direct connection to IP addresses (if the address is in this format)
2) The server does not recognize the address
3) The server does not forward calls beyond its own domain
4) The server does not support the chosen codec
5) The called device does not support the chosen codec
6) The address is a POTS telephone number, and POTS interworking is not supported
7) The address is a POTS telephone number, and no credit is available (most services charge for this)

Advanced N/ACIP Topics

The basic entries provided will allow support for the vast majority of N/ACIP SIP based applications. But there are inevitably situations where the defaults don't work, and we've provided some advanced options that can help. As always, these options are located in the Systems Settings and can be made visible by selecting the **Advanced** box.

1) **IP Port -** Universally, SIP connections are supposed to use UDP port 5060 to negotiate calls between devices (and between servers and devices). Note this is only the negotiation channel--actual audio data is passed on the RTP ports. Changing this port number will change which incoming ports are used to initiate connections, and to which ports connection requests are sent. Obviously, the change must be made on both devices, and this change will essentially make your codec incompatible with industry-standard VoIP devices.

2) **RTP Port -** This is one of two port numbers used for audio data transfer (the port number directly above this is used as well). Because this port number is negotiated at the beginning of a call (over the IP port), this port may be changed without breaking compatibility. Note that many SIP standard devices use port 5004 for this function. Due to the negotiation, it is not important that these numbers match on each end. Changing this port to 5004 can actually have an adverse effect, since 5004 is the default port for other services on Comrex codecs.

3) **Public IP Override -** See the next section, *SIP Troubleshooting*, for more information on this option.

4) **Use STUN Server -** See the next section, *SIP Troubleshooting*, for more information on this option.

5) **SIP Proxy Keepalive -** Only applies to *Registered* mode. This variable determines how often the codec "phones home" if registered with a SIP server. It's important that the codec periodically "ping" the server, so the server can find the codec for incoming calls. It can be adjusted primarily to compensate for firewall routers that have shorter or longer binding timings, i.e. the router may have a tendency to "forget" that the codec is ready to accept incoming calls and block them.

6) **SIP Domain -** Only applies to *Registered* mode. This is the name of the network controlled by the SIP server. This parameter must be passed by the codec to the server. Under most circumstances, this is the same as the server/proxy address, and if this field is not populated, that is the default. If, for some reason, the domain is different than the server/proxy address then this field is used.

SIP TROUBLESHOOTING

In a nutshell, SIP establishes a communication channel from the calling device to the called device (or server) on port 5060. All handshaking takes place over this channel, and a separate pair of channels is opened between the devices, one to handle the audio, and the other to handle call control. The original communication channel is terminated once the handshaking is complete. Note that firewalls must have all three ports open to allow calls to be established correctly. Also, port forwarding may be required to accept calls if your codec is behind a router.

The main area where SIP complicates matters is in how an audio channel gets established once the handshake channel is defined. In the common sense world, the call would be initiated to the destination IP address, then the called codec would extract the source IP address from the incoming data and return a channel to that address. In fact, that's how the default mode of Comrex codecs work, and it works well.

But SIP includes a separate "forward address" or "return address" field, and requires that a codec negotiating a call send to that address only. This is important in the case of having an intermediate server. And this works fine as long as each codec knows what its public IP address is.

OUTGOING CALL ISSUES

A unit making an outgoing call must populate the "return address" field. But any codec sitting behind a router has a private IP address, and has no idea what the public address is. So, naturally, it will put its private (e.g. 192.168.x.x style) address into that "return address" field. The called codec will dutifully attempt to connect to that address and undoubtedly fail, since that can't be reached from the Internet at large.

INCOMING CALL ISSUES

Incoming calls to codecs behind routers are complicated by the fact that ports on the router must be forwarded to the codec. In the case of SIP, this must be three discrete ports (For Comrex codecs these are UDP 5060, 5014 and 5015)<6014 and 6015 with 3.0 firmware>. And since even the "forward address" is negotiated in SIP, the incoming unit is likely to populate the "forward address" field with its private address as well.

Solutions

Many times the "return address" field issue is fixed by the SIP server (in *Registered* mode) and no compensation measures are necessary. Often, in fact, the server insists on acting as a "proxy" and handles all the traffic itself--outgoing and incoming streams are relayed directly by the server, solving any router issues.

But in point-to-point connections, this isn't possible. All is not lost here, since we can find some hacks to make this work. The first place to look is your router, since many modern routers are aware of this issue and have taken steps to relieve the pain. If your router supports a SIP Application Layer Gateway (ALG), then enabling this option can fix the issue. Essentially, the router will get smart enough to read your SIP handshake, find the outgoing address field, and replace it with your public IP. This is a pretty slick solution, but there may be environments when you are not aware whether this option is supported on your router, or have the ability to enable it. So on to solution two:

STUNning Success

Another technique for working around the SIP-Router issue is by using a protocol called STUN. This can be enabled in Comrex codecs in the **Advanced N/ACIP SIP** options and essentially allows for the codec to learn what its public IP address is. It does this by contacting a STUN server out on the Internet (the default one is maintained by Comrex) and simply asking. If this option is enabled, the codec itself will handle the address switching.

Be aware of the dreaded "battling workarounds" issue. In our simple description, we left out the fact that ports are being translated by the router as well as IP addresses. If the ALG-enabled router receives an unexpected result in the SIP address field (as it might if using STUN), it may not translate ports as expected, and it's likely that the call will fail. When in doubt, the best technique is to try a SIP call with STUN turned off, and if the return channel fails, try enabling STUN.

Fix of Last Resort

Finally, there's a brute-force option available on Comrex Codecs when STUN ports are blocked by a firewall, or it can't be used for some other reason. Under **Advanced System Settings**, a field is available called **Public IP Override**. Any address put into that field will be pasted into the address SIP field. So if you know what your public IP address is (can be gotten from many websites via a browser) you can manually paste it here. Keep in mind, this is often subject to change over time (and obviously if you use a different network) so it's important to remember this change has been made on your codec.

SECTION 17 ADVANCED TOPICS

QUESTIONS & ANSWERS

This section discusses some frequently asked questions (and possible solutions) encountered when setting up, configuring, troubleshooting and achieving optimum ACCESS performance.

Q: How do I choose which encoding algorithm to use?

A: ACCESS offers a very wide range of encoding algorithms. To some this may seem daunting. Here's a short guide and comparison chart on how to choose what's best for your application:

1) *Do I have lots and lots of bandwidth?* If you're running on an entirely unconstrained network like a campus LAN or local Wi-Fi, *Mono* or *Stereo Linear Mode* will offer the highest audio quality with lowest delay. If you're hitting the public Internet at any point in the link, however, avoid *Linear Mode*.

2) *Do I require interactivity?* If you need to chat back and forth across the link, choose one of our low delay algorithms like *BRIC-ULB*, *BRIC-HQ1* or *AAC-ELD*. The deciding factor between these algorithms is digital bandwidth — *BRIC-ULB* uses very little, *BRIC-HQ1* and *AAC-ELD* (optional upgrade) require more.

3) *Is audio quality the paramount concern? AAC* or *HE-AAC* (optional upgrades) are the best choices for applications that need excellent audio quality. If delay is also a concern, consider *AAC-ELD* (optional upgrade). If you are running on an unconstrained network and without the optional algorithms, *Linear PCM* would be a good choice.

4) *Am I running on a constrained network?* If your Internet pipe is subject to being throttled, use *BRIC-ULB* for mono voice audio and *BRIC-HQ2* for stereo voice or music. These algorithms offer the absolute highest quality in exchange for extremely low network bandwidth. If you have the optional AAC upgrade, *HE-AACv2* can also be a very effective, low network utilization option.

5) *Do I need to deliver two unrelated audio signals to the same location? BRIC-HQ1, AAC, HE-AAC* and *AAC-LD* (optional upgrade) offer *Dual Mono* options that allow uncorrelated signals (such as dual language broadcasts) to be combined to a single outgoing stream. Note: It isn't possible to send one stream to location A and one to location B. However, it is possible to send the combined stream to locations A and B and have them tap only their respective channels (although this can be a confusing solution subject to operator error).

Comparison Chart for ACCESS Codecs			
Required Bitrate	*Coding Delay*	*Audio Bandwidth*	**BRIC HQ1:** Sends good quality audio over narrow digital channels with low delay.
28 kb/s	55 ms	15 kHz	**A1 Mono**
42 kb/s	55 ms	15 kHz	**A2 Stereo**
56 kb/s	55 ms	15 kHz	**A3 Dual Mono** allows independent programming to be sent on both L&R channels
24 kb/s	55 ms	15 kHz	**A4 Mono 24Kb** restricted to 24 kbps coding rate
			BRIC HQ2: Sends excellent quality audio over narrow digital channels with moderate delay
24 kb/s	170 ms	15 kHz	**B1 Mono**
24 kb/s	170 ms	12 kHz	**B2 Mono 12Kb** reduced bandwidth with fewer coding artifacts
30 kb/s	170 ms	15 kHz	**B3 Stereo**
30 kb/s	170 ms	12 kHz	**B4 Stereo 12Kb** reduced bandwidth with fewer coding artifacts
24 kb/s	170 ms	15 kHz	**B5 Stereo 24Kb**
			BRIC ULB: For “worst case” networks - delivers 7kHz voice at ultra low bitrates with low delay (not recommended for music)
14 kb/s	49 ms	7 kHz	**C1 Mono** lowest bitrate of any BRIC algorithm
			Linear PCM: Delivers transparent audio with no compression and very low delay - for use on high throughput networks.
768 kb/s	19 ms	20 kHz	**F1 Mono**
1536 kb/s	19 ms	20 kHz	**F2 Dual Mono**
512 kb/s	19 ms	15 kHz	**F3 Mono**
1024 kb/s	19 ms	15 kHz	**F4 Dual Mono**
			FLAC: Free Lossless Audio Compression provides transparent audio while conserving bandwidth. FLAC bitrate is variable and based on audio input.
~540 kb/s	26 ms	20 kHz	**K1 Mono**
~1080 kb/s	26 ms	20 kHz	**K2 Dual Mono**
~360 kb/s	26 ms	15 kHz	**K3 Mono**
~720 kb/s	26 ms	15 kHz	**K4 Dual Mono**
			VoIP: G.711 and G.722 coding algorithms for compatibility with SIP-style VoIP phones.
64 kb/s	35 ms	3 kHz	**X1 G.711 a-law**
64 kb/s	35 ms	3 kHz	**X2 G.711 μ-law**
64 kb/s	35 ms	7 kHz	**X3 G.722**

Comparison Chart for AAC Codecs			
Required Bitrate	*Coding Delay*	*Audio Bandwidth*	**AAC:** Provides near transparent audio at relatively high data rates. Best used on non-constrained data networks - for situation where latency is not important.
64 kb/s	69 ms	20 kHz	**D1 Mono**
96 kb/s	69 ms	20 kHz	**D2 Stereo**
128 kb/s	69 ms	20 kHz	**D3 Dual Mono** allows independent programming to be sent on both L&R channels
128 kb/s	69 ms	20 kHz	**D4 Stereo 128Kb**
256 kb/s	69 ms	20 kHz	**D5 Dual Mono 256Kb** allows independent programming to be sent on both L&R channels
56 kb/s	69 ms	20kHz	**D6 Mono 56Kb**
96 kb/s	69 ms	20kHz	**D7 Mono 96Kb**
160 kb/s	69 ms	20kHz	**D8 Stereo 160Kb**
			HE-AAC: Provides near transparent audio at low data rates - for situations where latency is not important.
48 kb/s	144 ms	20 kHz	**E1 Mono**
64 kb/s	144 ms	20 kHz	**E2 Stereo**
96 kb/s	144 ms	20 kHz	**E3 Dual Mono** allows independent programming to be sent on both L&R channels
			HE-AAC V2: Provides medium quality HE-AAC implementation using Spectral Band Replication.
18 kb/s	209 ms	12 kHz	**G1 Mono 18Kb**
24 kb/s	268 ms	12 kHz	**G2 Stereo 24Kb** adds Parametric Stereo to SBR for higher quality audio at low data rate
32 kb/s	184 ms	20 kHz	**G4 Stereo 32Kb** adds Parametric Stereo to SBR for higher quality audio at low data rate
48 kb/s	210 ms	20 kHz	**G3 Stereo 48Kb** adds Parametric Stereo to SBR for higher quality audio at low data rate
56 kb/s	184 ms	20 kHz	**G5 Stereo 56Kb** adds Parametric Stereo to SBR for higher quality audio at low data rate
			AAC-LD: Requires higher data rates but provides near transparent voice or music with low delay.
96 kb/s	31 ms	20 kHz	**I1 Mono**
128 kb/s	31 ms	20 kHz	**I2 Stereo**
192 kb/s	31 ms	20 kHz	**I3 Dual Mono** allows independent programming to be sent on both L&R channels
256 kb/s	31 ms	20 kHz	**I4 Stereo 256Kb**
128 kb/s	31 ms	20 kHz	**I6 Mono 128Kb**
64 kb/s	31 ms	20 kHz	**I7 Mono 64Kb**
			AAC-ELD: combines the aspects of HE-AAC and AAC-LD to provide low delay, good audio quality and low bitrate. The best choice for low delay applications on the Internet.
48 kb/s	48 ms	20 kHz	**J1 Mono**
64 kb/s	48 ms	20 kHz	**J2 Stereo**
96 kb/s	48 ms	20 kHz	**J3 Dual Mono** allows independent programming to be sent on both L&R channels
24 kb/s	48 ms	20 kHz	**J4 Mono 24Kb**

Q: Can I make ACCESS maintain an IP connection regardless of network status?

A: Yes. First define your remote setting and apply a profile to it. Next go to the **System Settings Tab**, and pull down the menu labeled **Always Connect to Remote**. Once you select your remote here, a connection to the remote will be established and remain indefinitely.

Q: Can I get a remote indication that ACCESS is connected to someone?

A: Yes. Using the **System Settings Tab**, you can re-assign **Contact Closure Output #4** to trigger whenever the ACCESS front panel **Ready** light is lit, indicating a valid incoming connection. The function of **Contact Closure #4** will be changed in the following ways:

a) **Contact Closure #4** will no longer be available as an end-to-end signal.

b) Whenever ACCESS detects a valid incoming stream, it will trigger **CC #4** and maintain it until all valid connections stop.

Q: What steps should I take when I'm having connection problems with ACCESS?

A: There are several steps you can take to determine that cause of poor IP connection using ACCESS. The first step is to determine whether the problem is occurring in one direction or both. If in only one direction, take a look at network usage patterns on the local end of each ACCESS. If someone else on your LAN is downloading large files on the decoder side (or uploading large files on the encoder side) this may cause some performance issues. You may need to ask them to temporarily cease activity, or investigate a network router solution that will offer ACCESS priority over other traffic. Next, take a look at the **Status Tab** on the ACCESS that is decoding the faulty audio. Take a look at the jitter figure for your incoming connection. If this number is varying dramatically (good networks keep this figure below 50mS) then you may need to increase the **Local Delay Cushion** setting within the profile used to connect to that remote. Although it will increase your audio time delay, you may find increasing the cushion by 100-300mS or more will result in more stable connections, since the jitter buffer manager will no longer attempt to reduce delay by making the buffer smaller than the cushion.

Q: How can I optimize settings for EVDO, UMTS, or other wireless access?

A: Since there is typically already a substantial delay in these networks, it's often not a priority to keep ACCESS delay to the absolute minimum. Using the profile that you set up for the EVDO connection, enter the **Advanced Options**. Raise the **Frames/Packet** setting to 4 in both **Local** and **Remote Encoders**. This will reduce overall bandwidth and enhance reliability on many networks. You may also need to increase **Delay Cushion** on the non-wireless decode side as described in the previous answer.

Q: I'm paying for my network bandwidth by the megabyte. How can I conserve?

A: Set both **Local** and **Remote** encoders (in the profile) to *BRIC-ULB*, which uses by far the lowest amount of data. While setting the profile, click the **Advanced Options** and set both **Local** and **Return Frames per Packet** setting to 4. This will decrease overhead and preserve bandwidth. Finally, if you don't require audio in both directions, disable the return channel by turning off the **Remote Transmitter** in the profile. As a guide, an ACCESS set this way will average about 8 minutes of talk time per megabyte in each direction.

Q: How can I change modem parameters like dial-tone-detect and ring cadence detection?

A: Contact Comrex for more info on this.

Q: I notice in the Advanced Options that I can change my streaming from UDP to TCP. Should I?

A: Not if you want the best overall performance. ACCESS is optimized in terms of data rate, stability and delay to use UDP. TCP mode increases overhead and delay, and is included only for environments where UDP is hopelessly blocked by a firewall. ACCESS decoders do listen to both TCP and UDP ports and choose whichever arrives first. If an ACCESS gets an incoming TCP connection, it will establish TCP in the other direction automatically. One other note for use with TCP — most of the information presented on the **Statistics Tab** is generated by the UDP functionality, so you won't see much here using TCP.

Q: My IT guy has apparently had way too much coffee because his face is all red and he's running around yelling something about Sarbanes/Oxley and crashing the corporate network. Is there something I can give him to make him feel better about the security of the network and his life in general?

A: Why, yes! We've created a special document called "Information for IT Managers" which was written specifically to help keep the blood pressure and stress levels of IT managers within normal tolerance. It can be found in the *Appendix B* of this manual or in the Support section of our website at www.comrex.com

EBU3326, SIP, STUN and IP Compatibility

Everything you always wanted to know (about EBU3326, SIP, STUN, and compatibility with IP codecs) but were afraid to ask.

by the Codec Answer Guy

This paper describes everything you need to know about making ACCESS and BRIC-Link codecs work with other vendors. We're diving into some deep tech here, so grab that last cup of coffee in the pot and hang the "Do Not Disturb" sign the office door. We're going to take a leap here and assume familiarity with concepts like public and private IP addresses, NAT routers and application-specific port numbers used by IP data. If this isn't the case, a good overview is available in our product manuals.

What is all this about?

Comrex codecs (and many other brands) have a set of nifty protocols that allow easy IP connections between units. So easy, in fact, that we don't even recommend reading this paper unless you have a need to communicate with non-Comrex products.

But many users are concerned about getting "locked in" to a certain codec brand. So an international committee was formed by the European Broadcast Union called N/ACIP to hammer out a common protocol to interconnect codec brands. This committee resulted in the establishment of EBU3326, a technical document describing how best to achieve this goal.

EBU3326 by and large establishes a set of features each codec should support, then leaves most of the heavy lifting to other, previously established standards like SIP (IETF RFC 3261). Topics not covered (yet) by EBU3326

include things like carrying ancillary data and contact closures from end-to-end, codec remote control and monitoring, and NAT traversal, which at this point are still left to the individual manufacturer's discretion. So if these topics are important to your application, it's best to stick to a single codec vendor and their proprietary protocols.

More about EBU3326

The saying goes that a camel is "a horse built by a committee", and true to form EBU3326 has some elements that make things frustrating and complex. The document defines several mandatory encoding algorithms, and the transport layer that could be used on them for compatibility*. For the most part, the transports are straightforward and reasonable to implement and should interoperate.

It should be noted that several mandatory algorithms like G.711, G.722, and MP2 were included which provide little benefit to IP codec customers. Comrex has declined to include MP2, which makes our codecs technically in violation of the standard.

But the most complex part of the standard was the decision on how to arrange Session Initialization, which is the handshake that takes place at the start of an IP codec call. The most commonly used protocol is called SIP, which is used extensively by VoIP phones and therefore was a logical choice. But SIP isn't terribly simple and has some drawbacks which will affect codec operation. We've built into Comrex codecs several work-arounds to reduce these limitations, but understanding how best to utilize them requires that you understand what the limitations are.

Sipping Slowly

In a nutshell, SIP establishes a communication channel from the calling device to the called device* on port 5060. All handshaking takes place over this channel, and a separate pair of channels is opened between the devices, one to handle the audio, and the other to handle call control. The original communication channel is terminated once the handshaking is complete. Note that firewalls must have all three ports open to allow calls to be established correctly. Also, port forwarding may be required to accept calls if your codec is behind a router.

*In reality, most VoIP calls involve a server used as an intermediary for the

handshaking. But we believe most codec calls will be handled directly, and SIP supports both techniques, so we'll ignore the topic of a SIP server here.

The main area where SIP complicates matters is in how an audio channel gets established once the handshake channel is defined. In the common sense world, the call would be initiated to the destination IP address, then the called codec would extract the source IP address from the incoming data and return a channel to that address. In fact, that's how the default mode of Comrex codecs work, and it works well.

But SIP includes a separate "forward address" or "return address" field, and requires that a codec negotiating a call send to that address only. And this works fine as long as each codec knows what it's public IP address is.

Outgoing Call Issues

A unit making an outgoing call must populate the "return address" field. But any codec sitting behind a router has a private IP address, and has no idea what the public address is. So, naturally, it will put its private (e.g. 192.168.x.x style) address into that "return address" field. The called codec will dutifully attempt to connect to that address and undoubtedly fail, since that can't be reached from the Internet at large.

Incoming Call Issues

Incoming calls to codecs behind routers are complicated by the fact that ports on the router must be forwarded to the codec. In the case of SIP, this must be three discrete ports (For Comrex codecs these are UDP 5060, 5014 and 5015)<6014 and 6015 with 3.0 firmware>. And since even the "forward address" is negotiated in SIP, the incoming unit is likely to populate the "forward address" field with it' private address as well.

So to clarify, because SIP has this requirement, it makes things more difficult and complex when connecting from or to behind a router than the default Comrex connection mode.

Work-Arounds

All is not lost here, since we can find some hacks to make this work. The first place to look is your router, since many modern routers are aware of

this issue and have taken steps to relieve the pain. If your router supports a SIP Application Layer Gateway (ALG), then enabling this option can fix the issue. Essentially, the router will get smart enough to read your SIP handshake, find the outgoing "address" field, and replace it with your public IP. This is a pretty slick solution, but there may be environments when you are not aware whether this option is supported on your router, or have the ability to enable it. So on to solution two;

STUNning Success

Another technique for working around the SIP-Router issue is by using a protocol called STUN. This can be enabled in Comrex codecs, and essentially allows for the codec to learn what its public IP address is. It does this by contacting a STUN server out on the Internet (the default one is maintained by Comrex) and simply asking. If this option is enabled, the codec itself will handle the "address" switcheroo.

Be aware of the dreaded "battling workarounds" issue. In our simple description, we left out the fact that ports are being translated by the router as well as IP addresses. If the ALG-enabled router receives an unexpected result in the SIP "address" field (as it might if using STUN), it may not translate ports as expected, and it's likely that the call will fail. When in doubt, the best technique is to try a SIP call with STUN turned off, and if the return channel fails, try enabling STUN.

Fix of Last Resort

Finally, there's a brute-force option available on Comrex Codecs when STUN ports are blocked by a firewall, or it can't be used for some other reason. Under Advanced System Settings, a field is available called "Public IP Override". Any address put into that field will be pasted into the "address" SIP field. So if you know what your public IP address is (can be gotten from many websites via a browser) you can manually paste it here. Keep in mind, this is often subject to change over time (and obviously if you use a different network) so it's important to remember this change has been made on your codec.

SECTION 18 LICENSE AND WARRANTY DISCLOSURES FOR COMREX ACCESS

LICENSE

MPEG-4 audio coding technology licensed by Fraunhofer IIS
http://www.iis.fraunhofer.de/amm/

IIS
Fraunhofer Institut
Integrierte Schaltungen

ACCESS uses proprietary and open-source software programs. Some of the open-source programs are licensed under the Gnu Public License (GPL). For more information on GPL see http://www.gnu.org.

As per the GPL, source code for this software is available on request from Comrex on CD-ROM or other electronic format. To obtain this software please contact our support department at +1 978 784 1776. We retain the right to charge a small handling fee for distribution of this software.

ACCESS makes use of open-source and/or free software with the following copyright restrictions:

ncurses
Copyright (c) 1998,1999,2000,2001 Free Software Foundation, Inc.
See further Copyright notice below

dropbear
Copyright (c) 2002-2004 Matt Johnston
Portions copyright (c) 2004 Mihnea Stoenescu
All rights reserved.
See further Copyright notice below

libxml2
Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.
See Further Copyright notice below

Import code in **keyimport.c** is modified from PuTTY's import.c, licensed as follows:

PuTTY is copyright 1997-2003 Simon Tatham

Portions copyright Robert de Bath, Joris van Rantwijk, Delian Delchev, Andreas Schultz, Jeroen Massar, Wez Furlong, Nicolas Barry, Justin Bradford, and CORE SDI S.A.

Further copyright notice for ncurses, dropbear PuTTY and libxml2

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.
Libpcap
tcpdump

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. The names of the authors may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED "AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

WARRANTY

All Equipment manufactured by Comrex Corporation is warranted by Comrex against defects in material and workmanship for one year from the date of original purchase, as verified by the return of the warranty registration card. During the warranty period, we will repair or, at our option, replace at no charge a product that proves to be defective, provided you obtain a return authorization from Comrex and return the product, shipping prepaid to Comrex Corporation, 19 Pine Rd, Devens MA 01434 USA. For return authorization, contact Comrex at 800-237-1776 or 978-784-1776 or email techies@comrex.com.

This warranty does not apply if the product has been damaged by accident or misuse or as a result of service or modification performed by anyone other than Comrex Corporation.

The next two paragraphs apply to all software contained in this product:

WITH THE EXCEPTION OF THE WARRANTIES SET FORTH ABOVE, THE PRODUCT (MEANS COLLECTIVELY THE HARDWARE AND SOFTWARE COMPONENTS) IS PROVIDED STRICTLY "AS-IS." COMREX CORPORATION AND ITS SUPPLIERS MAKE NO WARRANTY, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR WARRANTY AGAINST LATENT DEFECTS. COMREX CORPORATION AND ITS SUPPLIERS DO NOT WARRANT THAT THE PRODUCT IS ERROR-FREE, THAT ALL ERRORS MAY BE DETECTED OR CORRECTED, OR THAT THE USE OF THE PRODUCT WILL BE UNINTERRUPTED. IN NO EVENT WILL COMREX CORPORATION AND ITS SUPPLIERS BE LIABLE FOR INDIRECT, INCIDENTAL, SPECIAL OR CONSEQUENTIAL DAMAGE RESULTING FROM THE USE OF THE PRODUCT INCLUDING LOSS OF PROFITS, LOSS OF SAVINGS, LOSS OF USE OR INTERRUPTION OF BUSINESS EVEN IF COMREX CORPORATION OR ANY OF ITS SUPPLIERS HAS BEEN ADVISED OF THE POSSIBILITY OF SAME. IN NO EVENT SHALL COMREX CORPORATION AND/OR ITS SUPPLIERS' TOTAL LIABILITY TO YOU REGARDLESS OF THE FORM OF ACTION EXCEED THE AMOUNT YOU PAID AS PART OF THE PURCHASE PRICE OF THIS PRODUCT. COMREX CORPORATION AND ITS SUPPLIERS MAKE NO WARRANTY, EITHER EXPRESSED OR IMPLIED, THAT ANY USE OF THE PRODUCT WILL BE FREE FROM INFRINGEMENT OF PATENTS, COPYRIGHTS, OR ANY OTHER THIRD PARTY'S INTELLECTUAL PROPERTY RIGHTS.

THE SOFTWARE OWNED BY COMREX CORPORATION OR BY ITS SUPPLIERS RESIDING IN OR OTHERWISE ASSOCIATED WITH THIS PRODUCT ARE PROTECTED UNDER COPYRIGHT LAW AND INTERNATIONAL TREATIES. UNAUTHORIZED REVERSE ENGINEERING, REPRODUCTION AND/OR DISTRIBUTION OF THE PRODUCT OR ANY PORTION THEREOF, IS STRICTLY PROHIBITED AND MAY RESULT IN CIVIL AND CRIMINAL SANCTIONS, AND WILL BE PROSECUTED TO THE FULL EXTENT OF THE LAW. COMREX CORPORATION AND ITS SUPPLIERS OWNS AND SHALL RETAIN ALL RIGHT, TITLE AND INTEREST IN AND TO ANY SOFTWARE SUPPLIED TO YOU IN AND AS PART OF THE PRODUCT AND ALL INTELLECTUAL PROPERTY RIGHTS RELATED THERETO. THE SALE OF THE PRODUCT SHALL NOT BE CONSTRUED IN ANY MANNER AS TRANSFERRING ANY RIGHT OF OWNERSHIP IN ANY SUCH SOFTWARE.

SECTION 19 ACCESS/BRIC-LINK TRAVERSAL SERVER USE DISCLAIMER

TRAVERSAL SERVER DISCLAIMER

You have purchased a product from Comrex that uses the Switchboard TS (Traversal Server) to provide the ability to locate Comrex hardware via the Internet and to aid in the making of connections when certain types of NAT routers are involved in the link. Switchboard TS consists of two distinct elements: The firmware that functions within the codec hardware to enable use of the function, and a server deployed on the Internet which provides the services to the codec hardware.

The purchase you have made entitles you only to the firmware elements within your codec that utilize these functions. The functions of Switchboard TS, as implemented in your codec, are warranted to work as described (according to standard Comrex warranty terms found in your User Manual) when used with a properly functioning Traversal Server deployed on the Internet.

Comrex has deployed and provided you account details for a Switchboard TS account on our server, located at http://switchboard.comrex.com.

Comrex provides this service, free of charge and at will. As such, Comrex offers no warranty as to availability of this server or of its function. Comrex reserves the right to discontinue availability of this service at any time. Comrex also reserves the right to remove any account from the server at http://switchboard.comrex.com at any time for any reason. In no way shall Comrex be liable for this server's malfunction, lack of availability or any resultant loss therein.

The software that runs the Comrex Traversal Server on the Internet is available from Comrex in an executable format, free of charge, with basic instructions on how to set it up. The address of the server used for these functions is configurable in the codec firmware. If you wish to deploy your own Traversal Server, contact Comrex for details on obtaining this software.

Comrex is not liable for training or support in setting up a TS server, and the software is available without warrantee or guarantee of suitability of any kind.

SECTION 20 CONFORMITY AND REGULATORY INFORMATION

SUPPLIERS' DECLARATION OF CONFORMITY

Place of Issue: Devens, Massachusetts

Date of Issue: January 23, 2006

Comrex Corporation, located at 19 Pine Road, Devens, MA in the United States of America hereby certifies that the Comrex ACCESS Rack bearing identification number US:DXDMD01BACCRK complies with the Federal Communications Commission's ("FCC") Rules and Regulations 47 CFR Part 68, and the Administrative Council on Terminal Attachments ("ACTA")-adopted technical criteria TIA/EIA/IS-968, Telecommunications – Telephone Terminal Equipment – Technical Requirements for Connection of Terminal Equipment To the Telephone Network, July 2001.

Thomas O. Hartnett, Vice President, Comrex Corporation

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

EC DECLARATION OF CONFORMITY FOR R&TTE DIRECTIVE

We:

Manufacturer's Name: Comrex Corporation

Manufacturer's Address: 19 Pine Road
Devens, MA 01434

hereby declare on our sole responsibility that the product:

Comrex ACCESS Rack
Digital Audio Codec

to which this declaration relates is in conformity with the essential requirements and other relevant requirements of the R&TTE Directive (1999/5/EC). This product is compliant with the following standards and other normative documents:

European EMC Directive (89/336/EEC)
EN 55022:1998/A1:2000, Class A Conducted and Radiated Emissions
EN55024: 1998/A1:2001/A2:2003 (Immunity, ITE Equipment)
Low Voltage Directive (72/23/EEC)
EN 60950-1: 2001

Information regarding configuration of this equipment for operation on the telephone networks of the EC countries may be found in the Comrex ACCESS Rack product manual.

Contact person: Thomas O. Hartnett, V.P., Engineering

Signed:________________________________

Date: 23 January 2006

U.S. and Canadian Regulatory Information for the ACCESS Rack

This equipment complies with Part 68 of the FCC rules and the requirements adopted by the ACTA, as well as the applicable Industry Canada technical specifications. On the bottom of this equipment is a label that contains, among other information, a product identifier in the format US: DXDMD01BACCRK. If requested, this number must be provided to a U.S. telephone company.

Telephone line connections to the Comrex ACCESS Rack are made via an RJ11C jack. A plug and jack used to connect this equipment to the premises wiring and telephone network must comply with the applicable FCC Part 68 rules and requirements adopted by the ACTA. A compliant telephone cord and modular plug is provided with this product. It is designed to be connected to a compatible modular jack that is also compliant. See installation instructions for details.

The REN is used to determine the number of devices that may be connected to a telephone line. Excessive RENs on a telephone line may result in the devices not ringing in response to an incoming call. The sum of RENs should not exceed five (5.0). To be certain of the number of devices that may be connected to a line, as determined by the total RENs, contact the local telephone company. The REN for the Comrex ACCESS Rack is 0.1, and is shown as the digits represented by ## in the product identifier US: DXDMD###ACCRK.

If the Comrex ACCESS Rack causes harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also, you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

The telephone company may make changes in its facilities, equipment, operations, or procedures that could affect the operation of this equipment. If this happens the telephone company will provide advance notice in order for you to make necessary modifications to maintain uninterrupted service.

If trouble is experienced with the Comrex ACCESS Rack, please contact Comrex Corporation at 978-784-1776 for repair or warranty information. If the equipment is causing harm to the telephone network, the telephone company may request that you disconnect the equipment until the problem is solved.

No user serviceable parts are contained in this product. If damage or malfunction occurs, contact Comrex Corporation for instructions on its repair or return.

Connection to party line service is subject to state tariffs. Contact the state public utility commission, public service commission or corporation commission for information. This equipment cannot be used on telephone company provided coin service.

If you have specially wired alarm equipment connected to the telephone line, ensure the installation of the Comrex ACCESS Rack does not disable your alarm equipment. If you have questions about what will disable alarm equipment, consult your telephone company or a qualified installer.

Appendix A IP Compatibility

IP compatibility using ACCESS firmware 2.3 and later offers several modes that allow compatibility with other IP coding devices. These compatible modes rely on the AAC family of algorithms. All ACCESS with firmware 2.3 are capable of *decoding* streams sent to them using these devices. In order to *encode* streams that are compatible with these devices, the optional AAC upgrade must be installed on the ACCESS. Contact Comrex for more details.

The ACCESS is capable of encoding and decoding a choice of three different types of non-ACCESS streams: Standard RTP, Luci Live and Zephyr Xstream. The choice is exclusive i.e. you must set the ACCESS specifically for the type of stream you wish to be compatible with, and you will remain incompatible with the other two types until you change it. This setting has no effect on normal ACCESS BRIC/POTS/AAC functions, which continue to operate as before.

1) Luci Live — This PDA/PC-based software allows real-time streaming over IP links. As of version 1.2, Luci Live includes AAC and HE-AAC in addition to the default MP2 algorithm. ACCESS can communicate with Luci Live only in Luci's AAC modes. Note: The free demo available from Luci does not incorporate the AAC functions; you must have a licensed and registered copy to use AAC.
To communicate with a Luci Live device:

a) Initial Setup — This will define all Standard RTP connections to be Luci Compatible

i) ACCESS Rack — On the **System Settings Tab**, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, choose **Luci Live**.

ii) ACCESS Portable — Choose **Configure** then **System Settings** on the display. Under **Standard RTP Settings** select **RTP Compatibility Mode** and choose **Luci Live**.

b) Incoming Connections — Luci Live sends either an AAC or HE-AAC stream to the ACCESS on UDP port 5004. These streams will be automatically decoded. By default, a return channel of AAC 56kb/s mono is returned to the Luci Live product. The return channel may be altered to any Luci-compatible mode in the **Systems Setting** section. ACCESS that do not have the AAC upgrade applied will not create a return channel.

c) Outgoing Connections (ACCESS AAC Option required) — Build a profile using the **Profile Manager** on either the ACCESS Rack or Portable and select a *Channel Mode* of **Standard RTP**. Then choose a Luci-compatible encoder for the outgoing call. The Luci software will control what type of stream, if any, is returned to the ACCESS.

2) Zephyr Xstream — Xstream Firmware version 3.2.0 and higher support an "RTP Push" function that is compatible with ACCESS in some modes. ACCESS is not currently compatible with the Xstream's HTTP and SIP streaming functions. There are several limitations imposed by the Xstream when using the RTP Push function:

-- On the Xstream, only AAC and MP3 coding are available in this mode, and ACCESS is only compatible with the AAC mode
-- The Xstream uses downsampling in modes below 96Kb/s, which is not supported by ACCESS.
-- In order for an Xstream to decode an ACCESS stream, the default decoder setting must be changed from <Auto> to <AAC> in the codec menu of the Xstream.

To communicate with a Zephyr Xstream:

a) Initial Setup — This will define all Standard RTP connections to be Xstream Compatible.

i) ACCESS Rack — On the **System Settings Tab**, open the **Standard RTP Settings** option and choose **RTP Compatibility Mode**. On the pull-down box, select **Zephyr Xstream**.
ii) ACCESS Portable — Choose **Configure** then **System Settings** on the display. Under **Standard RTP Settings** select **RTP Compatibility Mode** and choose **Zephyr Xstream**.

b) Incoming Connections— Zephyr Xstream sends an AAC stream to the ACCESS on UDP port 9150. These streams will be automatically decoded. By default, a return channel of AAC 96kb/s mono is returned to the Xstream. The return channel may be altered to any Xstream-compatible mode in the **Systems Setting** section. ACCESS that do not have the AAC upgrade applied will not create a return channel.

c) Outgoing Connections (ACCESS AAC Option required) — Build a profile using the **Profile Manager** on either the ACCESS Rack or Portable and select a *Channel Mode* of **Standard RTP**. Then choose an Xstream-compatible encoder for the outgoing call. The Xstream will control what type of stream, if any, is returned to the ACCESS.

3) Standard RTP — This mode is set to receive a basic, unformatted AAC stream within a standard RTP/UDP structure. At present, this mode does not offer compatibility with other industry devices.

APPENDIX B INFORMATION FOR IT MANAGERS

The purpose of this appendix is to describe all open ports and services available on the Comrex ACCESS. If a service is not mentioned here, it is disabled by default.

The Comrex ACCESS is a device designed to move real-time, wideband audio over IP networks. The main network interface is 10/100 10baseT Ethernet.

The device contains an optimized version of the 2.6 Linux kernel. The IP parameters are set using a GUI that requires attachment of a keyboard and VGA monitor to the device.

Alternately, during the first five minutes of power up, the IP parameters may be set by a PC on the local LAN using a proprietary broadcast UDP protocol. Comrex provides the Device Manager application to perform this function on the local PC. After five minutes of operation, this function is disabled.

Firmware updates to the device are installed using the **Device Manager** utility software. This update process is password protected and done via XML over TCP port 8080. In addition to the password protection, the update data itself must have a valid cryptographic signature from Comrex, or else it is rejected. In order for the unit to be remotely updated, TCP port 8080 must be forwarded to the device. Alternately, updates can be initiated from any local PC using the **Device Manager** application.

In its most commonly used mode, the ACCESS codec delivers an RTP/UDP stream from source port 9000 to destination port 9000 by default. By default it listens for incoming RTP/UDP streams on port 9000. To use the default mode, only UDP 9000 needs to be forwarded to the device.

Alternately, the device can be configured to deliver a similar TCP-based stream on TCP port 9000. By default, the device listens for incoming TCP streams on TCP 9000. This function may be disabled. The source port of TCP streams is ephemeral, and, if an incoming stream is detected, one will be returned to the ephemeral port.

The device also supports transmitting and receiving UDP multicast streams, using UDP port 9002 unless another port is specified by the user. This is not enabled by default, and a configuration must be explicitly created and connected on both ends for this function. Multicast streams are inherently unidirectional, and the configured port must be forwarded to the device on the receiving end. The multicast TTL value defaults to 1 (for in-network multicasting), but may be changed to any valid TTL by the user.

Outgoing ports and incoming ports may be altered via the **User Interface**.

For compatibility with other industry devices, the ACCESS also listens for incoming streams (and can place outgoing streams) on UDP 5004 and 9150. The device also listens for incoming SIP connections on UDP port 5060, and in the case of successful negotiation will transfer audio on UDP ports 5014 and 5015<6014 and 6015 with 3.0 firmware>. These ports may be changed via the user interface, and these functions may be disabled.

The device has the ability to act as a streaming server, accepting TCP connections on port 8000 and delivering streaming data. This function is disabled by default, and the port number may be changed.

The device has an optional STUN server and directory download function (Switchboard TS). In order for this function to work, the device must be allowed to create an outgoing TCP socket from port 8082. As part of the STUN protocol, outgoing requests may be made on UDP ports 3478 and 3479.

By default, the device serves as an SSH host on TCP port 22. Only SSH clients with an authorized DSA key can access SSH services on the device. Other forms of authentication are disabled. This key is kept confidentially by Comrex for factory diagnostics only. SSH services may be disabled completely via the user interface.

Under normal operation, the device is controlled by a networked computer via a web page served from the device on the standard HTTP port 80 (TCP). This page requires Adobe Flash Player on the browser; and the Flash plugin establishes a TCP connection back to the device on the XML port 8080. Both of these ports are required for the remote UI to function, and the port assignments are configurable. These services may be disabled by the user interface, but this will disable both the remote GUI and the on-line updater. TCP Port 8080 is also used by the optional Remote Control software.

The device will respond to standard ICMP requests.

Appendix C Using ACCESS on Unidirectional Networks

Under most circumstances, ACCESS requires an IP path in both directions for successful connections, even when audio is being sent only one-way. For networks that provide data only in one direction, it is possible to use *Standard RTP* mode to establish and maintain these links. This section describes how to set that up.

The following setting applies to both codecs in the link (encoder and decoder):

The codec has several compatibility modes under the *Standard RTP* channel mode. The units default to a mode that is compatible with the Luci Live PC-based encoder. This must be changed on both codecs.

1) On the ACCESS Rack, enter the *Web-based User Interface* and choose the **System Settings** tab. On the ACCESS Portable choose **Configure > System Settings**
2) Find the **Advanced** tick-box and check it
3) Find **Standard RTP Settings** and choose to edit the **RTP Compatibility mode**.
4) Change this setting to **Standard** and click **Apply** (or **Save** on ACCESS Portable).

Decode Side Settings Only

Also under **Advanced Standard RTP Settings**, find the **Return Channel Enable** entry. Disable the return channel and click **Apply** (or **Save** on ACCESS Portable). This will make sure that no channel will be set up in the direction to the encoder.

Encode Side Settings Only

Obviously, connections of this type must be established from the encoding side of the link. So you'll need to build a new Profile that uses the **Standard RTP** channel mode under the Profile Editor. Choose your outgoing encoder along with any other special attributes in the profile editor. Name the Profile something descriptive like "Simplex".

Next, create your outgoing remote entry in the address book. Apply the new profile to that entry. Any connection made with that entry will connect in a unidirectional fashion.

FULL-TIME OR TRIGGERED CONNECTIONS

A remote entry using a unidirectional profile can still utilize the tools required for automatic connection.

To set up a connection to be "always active" (i.e. reconnect in the case of power outage or network failure), choose that connection on the **System Settings Tab** as the **Always Connect To** location.

To trigger the connection when an external contact is closed, choose the connection under one of the **Contact Closure** settings on the **System Settings Tab**.

Appendix D Specifications

Connections

Power: IEC 530 Inlet
Analog Line In Left/Digital AES3 In:
Analog: 3-pin XLR female, pin 1 ground, pin 2 +, pin 3 –
Digital: 3-pin XLR female, pin 1 ground, pin 2 data +, pin 3 data –
AES 3 Output: 3-pin XLR male, pin 1 ground, pin 2 data +, pin 3 data –
POTS/PSTN: 6-pin "RJ-11" modular jack, pin 3 tip, pin 4 ring
Contact Closures: 9-pin "D" male, pinout in Section 2
PS/2 Keyboard/Mouse: 6-pin mini-DIN female, for PS/2 Keyboard/Mouse
Serial (w/adapter): 9-pin "D" female, RS-232 pinout
Monitor: 15-pin "D" female, VGA monitor pinout
USB (2): USB Type A
Ethernet: 8-pin modular, 100BASE-T wiring

Audio Specifications

Line Inputs
- *Type*: Balanced
- *Impedance*: 50k Ohms (pins 2-3)
- *Level*: 0 dBu nominal, +20 dBu max

Line Outputs
- *Type*: Balanced
- *Impedance*: 100 Ohms (pins 2-3)
- *Level*: 0 dBu nominal, +20 dBu max

Frequency Response: Varies with algorithms, see descriptions.

Power

Voltage: 90-264 VAC, 50-60 Hz
Power: 50 Watts (120 VAC, 60 Hz), 65 Watts (240 VAC, 50 Hz)

Physical

Dimensions: 19" W (48.3 cm), 9.75" D (24.8 cm), 1.75" H (4.45 cm)
Weight: Unit alone: 8.6 lb (3.9 kg)
Shipping: 15 lb (6.8 kg) with all peripherals and packing